

PCT/JP 00/07473
25.10.00

JP00/A373
日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

REC'D 10 NOV 2000	
WIPO	PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:

1999年10月25日

EW

出願番号
Application Number:

平成11年特許願第303142号

出願人
Applicant(s):

ソニー株式会社

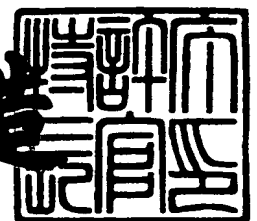
097857218

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2000年 9月18日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3075347

【書類名】 特許願
【整理番号】 9900793602
【提出日】 平成11年10月25日
【あて先】 特許庁長官 近藤 隆彦 殿
【国際特許分類】 G06F 19/00
【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 石黒 隆二

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 河上 達

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 田辺 充

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 江面 裕一

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 佐藤 一郎

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 海老原 宗毅

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100067736

【弁理士】

【氏名又は名称】 小池 晃

【選任した代理人】

【識別番号】 100086335

【弁理士】

【氏名又は名称】 田村 榮一

【選任した代理人】

【識別番号】 100096677

【弁理士】

【氏名又は名称】 伊賀 誠司

【手数料の表示】

【予納台帳番号】 019530

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707387

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 コンテンツ提供システム及びコンテンツ提供方法

【特許請求の範囲】

【請求項 1】 コンテンツデータを再生する再生プログラムを有するデータ処理装置と、上記データ処理装置から提供されたコンテンツデータを記憶媒体に格納して再生する可搬再生装置と、コンテンツデータをネットワークを介して上記データ処理装置に配信するコンテンツサーバとからなるコンテンツ提供システムにおいて、

上記データ処理装置は、

上記再生プログラムがインストールされた後に、第 1 のマスター鍵及び第 1 の認証鍵が上記再生プログラムに提供され、上記第 1 のマスター鍵を用いて当該装置に接続された外部記憶媒体に格納されたコンテンツデータを取得して保存し、上記再生プログラムがこの提供された第 1 の認証鍵及び第 1 のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行い、

上記再生プログラムが上記コンテンツサーバから配信されたコンテンツデータの送受信を上記可搬再生装置と行う場合には、上記第 1 のマスター鍵とは異なる第 2 のマスター鍵及び上記第 1 の認証鍵とは異なる第 2 の認証鍵がネットワークを介して提供され、この提供された第 2 のマスター鍵を用いて上記コンテンツサーバから提供されたコンテンツデータを取得して保存し、この提供された第 2 の認証鍵及び第 2 のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行うこと

を特徴とするコンテンツ提供システム。

【請求項 2】 上記可搬再生装置は、第 1 から第 i (i は 2 以上の整数) 世代まで世代更新されていく第 1 から第 i の認証鍵、及び、第 1 から第 i (i は 2 以上の整数) 世代まで世代更新されていく第 1 から第 i のマスター鍵を保持しており、

上記再生プログラムは、第 2 から第 i (i は 2 以上の整数) まで世代更新されていく第 2 から第 i の認証鍵、及び、第 2 から第 i (i は 2 以上の整数) まで世代更新されていく第 2 から第 i のマスター鍵がネットワークを介して提供され、

上記可搬再生装置と上記再生プログラムとは、同一世代の認証鍵を用いて相互認証を行うこと

を特徴とする請求項 1 記載のコンテンツ提供システム。

【請求項 3】 上記可搬再生装置は、上記再生プログラムと認証を行った際に、この再生プログラムが用いている世代よりも古い世代の認証鍵及びマスター鍵を用いている場合には、上記再生プログラムが用いている世代まで自己の認証鍵及びマスター鍵の世代を更新すること

を特徴とする請求項 2 記載のコンテンツ提供システム。

【請求項 4】 上記再生プログラムは、上記可搬再生装置と認証を行った際に、上記可搬再生装置が用いている世代よりも古い世代の認証鍵及びマスター鍵を用いている場合には、上記コンテンツサーバに鍵要求をして、上記可搬再生装置が用いている世代まで自己の認証鍵及びマスター鍵の世代を更新すること

を特徴とする請求項 2 記載のコンテンツ提供システム。

【請求項 5】 上記コンテンツサーバは、上記再生プログラムからアクセスされた際に、上記再生プログラムが用いている認証鍵の世代よりも新しい世代の認証鍵及びマスター鍵を上記再生プログラムに提供して、上記再生プログラムが用いている認証鍵の世代更新をすること

を特徴とする請求項 2 記載のコンテンツ提供システム。

【請求項 6】 コンテンツデータを再生する再生プログラムを有するデータ処理装置と、上記データ処理装置から提供されたコンテンツデータを記憶媒体に格納して再生する可搬再生装置とによりユーザにコンテンツデータを提供するコンテンツサーバとからなるコンテンツ提供方法において、

上記再生プログラムをインストールした後に、第 1 のマスター鍵及び第 1 の認証鍵が上記再生プログラムに提供され、上記第 1 のマスター鍵を用いて当該装置に接続された外部記憶媒体に格納されたコンテンツデータを取得して保存し、上記再生プログラムがこの提供された第 1 の認証鍵及び第 1 のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行い、

上記再生プログラムがコンテンツサーバから配信されたコンテンツデータの送受信を上記可搬再生装置と行う場合には、上記第 1 のマスター鍵とは異なる第 2

のマスター鍵及び上記第 1 の認証鍵とは異なる第 2 の認証鍵がネットワークを介して提供され、この提供された第 2 のマスター鍵を用いて上記コンテンツサーバから提供されたコンテンツデータを取得して保存し、この提供された第 2 の認証鍵及び第 2 のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行うこと

を特徴とするコンテンツ提供方法。

【請求項 7】 上記可搬再生装置が、第 1 から第 i (i は 2 以上の整数) 世代まで世代更新されていく第 1 から第 i の認証鍵、及び、第 1 から第 i (i は 2 以上の整数) 世代まで世代更新されていく第 1 から第 i のマスター鍵を保持しており、

上記再生プログラムは、第 2 から第 i (i は 2 以上の整数) まで世代更新されていく第 2 から第 i の認証鍵、及び、第 2 から第 i (i は 2 以上の整数) まで世代更新されていく第 2 から第 i のマスター鍵がネットワークを介して提供され、

上記可搬再生装置と上記再生プログラムとは、同一世代の認証鍵を用いて相互認証を行うこと

を特徴とする請求項 6 記載のコンテンツ提供方法。

【請求項 8】 上記可搬再生装置が、上記再生プログラムと認証を行った際に、この再生プログラムが用いている世代よりも古い世代の認証鍵及びマスター鍵を用いている場合には、上記再生プログラムが用いている世代まで自己の認証鍵及びマスター鍵の世代を更新すること

を特徴とする請求項 7 記載のコンテンツ提供方法。

【請求項 9】 上記再生プログラムが、上記可搬再生装置と認証を行った際に、上記可搬再生装置が用いている世代よりも古い世代の認証鍵及びマスター鍵を用いている場合には、上記コンテンツサーバに鍵要求をして、上記可搬再生装置が用いている世代まで自己の認証鍵及びマスター鍵の世代を更新すること

を特徴とする請求項 7 記載のコンテンツ提供方法。

【請求項 10】 上記コンテンツサーバが、上記再生プログラムからアクセスされた際に、上記再生プログラムが用いている認証鍵の世代よりも新しい世代の認証鍵及びマスター鍵を上記再生プログラムに提供して、上記再生プログラムが

用いている認証鍵の世代更新をすること

を特徴とする請求項 7 記載のコンテンツ提供方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

半導体メモリやメモリカード等を記憶媒体とした可搬再生装置にコンテンツデータを提供するコンテンツ提供システム及びコンテンツ提供方法に関するものである。

【0002】

【従来の技術】

近年、インターネットやケーブルテレビ等のネットワークを用いた音楽コンテンツのオンライン配信が実用化され始めた。

【0003】

このような音楽コンテンツの配信システムにおいては、コンテンツ配信業者は、音楽コンテンツをネットワークを介して配信する場合、例えば、Web上に音楽コンテンツを提供する。また、この音楽配信システムを利用するユーザは、自己のパーソナルコンピュータを用いて、コンテンツ配信業者が提供するWeb等にアクセスをして、所望の音楽コンテンツをダウンロードする。ユーザは、取得した音楽コンテンツを、例えば、パーソナルコンピュータ内のプレーヤアプリケーションにより再生したり、また、このパーソナルコンピュータと接続可能なポータブルデバイス等により再生する。

【0004】

ここで、コンテンツ提供業者は、そのコンテンツの著作権を管理しなければならない。そのため、コンテンツ配信業者は、インターネットを介してWeb上にアクセスしてきたユーザをID情報や暗証番号等で認識し、正当なユーザに対してのみに暗号化した音楽コンテンツを配信する。そして、その音楽コンテンツは、ユーザからは自由に参照できないような暗号鍵により鍵管理がされた状態で、パーソナルコンピュータ内のハードディスクに格納される。また、パーソナルコンピュータ内に格納された音楽コンテンツをポータブルデバイスに転送する場合

には、プレーヤアプリケーションとポータブルデバイスとの間で認証処理を行った後に、ポータブルデバイスが有する記憶媒体に音楽コンテンツが格納される。

【0005】

【発明が解決しようとする課題】

ところで、一般に、ポータブルデバイスやには、ネットワークから配信された音楽コンテンツのみならず、例えばCD等のメディアから音楽コンテンツをコピーすることもできる。

【0006】

ところが、従来、ポータブルデバイスとパーソナルコンピュータと間の認証の方式は、CD等のメディアからコピーされた音楽コンテンツのみを扱うプレーヤアプリケーションであろうが、ネットワークからダウンロードした音楽コンテンツを扱うプレーヤアプリケーションであろうが、特に区別がされず行われていた。

【0007】

そのため、例えば、なんらかの悪意を有する者により、ポータブルデバイスとパーソナルコンピュータとの認証鍵が破られた場合、CD等のメディアからコピーされた音楽コンテンツと、ネットワークを介して配信した音楽コンテンツとの両者ともに不正にコピーがされてしまう。

【0008】

特に、CD等のメディアの場合は、一般にメディアが販売された時に課金が終了している場合が主であるが、ネットワークを介して配信された音楽コンテンツは、例えば、再生をした回数や複製をした回数等に応じて課金等がされる場合があり、より強固な鍵管理が望まれる。

【0009】

本発明は、ネットワークを介して配信されたコンテンツデータの安全性を高めることができるコンテンツ提供システム及びコンテンツ提供方法を提供することを目的とする。

【0010】

【課題を解決するための手段】

本発明にかかるコンテンツ提供システムは、コンテンツデータを再生する再生プログラムを有するデータ処理装置と、上記データ処理装置から提供されたコンテンツデータを記憶媒体に格納して再生する可搬再生装置と、コンテンツデータをネットワークを介して上記データ処理装置に配信するコンテンツサーバとからなるコンテンツ提供システムにおいて、上記データ処理装置は、上記再生プログラムがインストールされた後に、第1のマスター鍵及び第1の認証鍵が上記再生プログラムに提供され、上記第1のマスター鍵を用いて当該装置に接続された外部記憶媒体に格納されたコンテンツデータを取得して保存し、上記再生プログラムがこの提供された第1の認証鍵及び第1のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行い、上記再生プログラムが上記コンテンツサーバから配信されたコンテンツデータの送受信を上記可搬再生装置と行う場合には、上記第1のマスター鍵とは異なる第2のマスター鍵及び上記第1の認証鍵とは異なる第2の認証鍵がネットワークを介して提供され、この提供された第2のマスター鍵を用いて上記コンテンツサーバから提供されたコンテンツデータを取得して保存し、この提供された第2の認証鍵及び第2のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行うことを特徴とする。

【0011】

コンテンツ提供システムでは、再生プログラムが、外部記憶媒体に格納されたコンテンツデータのみを取り扱う場合には、第1の認証鍵及び第1のマスター鍵を用いて、外部記憶媒体に格納されたコンテンツデータの保存及び可搬再生装置との認証を行う。再生プログラムが、ネットワークを介して提供されたコンテンツデータを取り扱う場合には、第1の認証鍵及び第1のマスター鍵を用いて、外部記憶媒体に格納されたコンテンツデータの保存及び可搬再生装置との認証を行う。第2の認証鍵及び第2のマスター鍵は、ネットワークを介して再生プログラムに提供され、第1の認証鍵及び第1のマスター鍵と異なる鍵となっている。

【0012】

本発明にかかるコンテンツ提供方法は、コンテンツデータを再生する再生プログラムを有するデータ処理装置と、上記データ処理装置から提供されたコンテンツデータを記憶媒体に格納して再生する可搬再生装置とによりユーザにコンテンツデータを提供するコンテンツサーバとからなるコンテンツ提供方法において、上記再生プログラムをインストールした後に、第1のマスター鍵及び第1の認証鍵が上記再生プログラムに提供され、上記第1のマスター鍵を用いて当該装置に接続された外部記憶媒体に格納されたコンテンツデータを取得して保存し、上記再生プログラムがこの提供された第1の認証鍵及び第1のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行い、上記再生プログラムがコンテンツサーバから配信されたコンテンツデータの送受信を上記可搬再生装置と行う場合には、上記第1のマスター鍵とは異なる第2のマスター鍵及び上記第1の認証鍵とは異なる第2の認証鍵がネットワークを介して提供され、この提供された第2のマスター鍵を用いて上記コンテンツサーバから提供されたコンテンツデータを取得して保存し、この提供された第2の認証鍵及び第2のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行うことを特徴とする。

【0013】

このコンテンツ提供方法では、再生プログラムが、外部記憶媒体に格納されたコンテンツデータのみを取り扱う場合には、第1の認証鍵及び第1のマスター鍵を用いて、外部記憶媒体に格納されたコンテンツデータの保存及び可搬再生装置との認証を行う。再生プログラムが、ネットワークを介して提供されたコンテンツデータを取り扱う場合には、第1の認証鍵及び第1のマスター鍵を用いて、外部記憶媒体に格納されたコンテンツデータの保存及び可搬再生装置との認証を行う。第2の認証鍵及び第2のマスター鍵は、ネットワークを介して再生プログラムに提供され、第1の認証鍵及び第1のマスター鍵と異なる鍵となっている。

【0014】

【発明の実施の形態】

(1) 音楽コンテンツ配信システムの全体構成

図 1 に本発明を適用した実施の形態の音楽コンテンツ配信システム 1 のシステム構成を示す。

【 0 0 1 5 】

本発明の実施の形態の音楽コンテンツ配信システム 1 は、この図 1 に示すように、インターネット等のネットワーク 2 を介して音楽コンテンツの提供等をする複数の EMD (Electrical Music Distribution) サーバと、各 EMD サーバから上記ネットワーク 2 を介して音楽コンテンツの配信を受けるパーソナルコンピュータ (以下、単にパソコンと略して称する。) 3 と、このパソコン 3 と USB (Universal Serial Bus) 等のインターフェース 4 により接続されこのパソコン 3 から音楽コンテンツが転送されて再生を行う携帯型の音楽再生機器である複数のポータブルデバイス (PD) とを備える構成となっている。

【 0 0 1 6 】

音楽コンテンツ配信システム 1 を構成している複数の EMD サーバには、例えば音楽提供会社 A から提供される音楽コンテンツを配信する EMD サーバ (A) 5 と、例えば音楽提供会社 B から提供される音楽コンテンツを配信する EMD サーバ (B) 6 と、例えば音楽提供会社 X から提供される音楽コンテンツを配信する EMD サーバ (X) 7 とがある。各 EMD サーバ 5, 6, 7 は、各社独自にラインナップがされた音楽コンテンツを、ユーザが持つパソコン 3 にネットワーク 2 を介して提供を行っている。また、各 EMD サーバ 5, 6, 7 では、音楽コンテンツの暗号化方式、利用条件 (Usage Rule) 情報のフォーマット、音楽コンテンツの圧縮方式、音楽コンテンツの課金方式等は、各社独自の方式が採用されており、各 EMD サーバ 5, 6, 7 では、それぞれ異なる方式により音楽コンテンツを配信している。

【 0 0 1 7 】

パソコン 3 には、音楽コンテンツの再生や管理等を行うためのアプリケーションソフトウェアとして、EMD サーバ (A) から音楽コンテンツの購入や管理を行う購入用アプリケーション (A) 1 1 と、EMD サーバ (B) から音楽コンテンツの購入や管理を行う購入用アプリケーション (B) 1 2 と、EMD サーバ (A) 5 から購入した音楽コンテンツの再生を行うデバイスドライバ (A) 1 3 と

、EMDサーバ(B) 6から購入した音楽コンテンツの再生を行うデバイスドライバ(B) 14とがインストールされている。また、パソコン3には、ハードディスク19内に格納されている全ての音楽コンテンツの包括的な管理を行う包括管理ユニット(X) 15がインストールされている。この包括管理ユニット(X) 15は、さらに、EMD用受信インターフェース16、EMD用送信インターフェース17、PD用ドライバ18により構成されている。

【0018】

ポータブルデバイス(A) 8は音楽提供会社Aに対応した専用の装置であり、ポータブルデバイス(B) 9は音楽提供会社Bに対応した専用の装置であり、ポータブルデバイス(X) 10は音楽提供会社Xに対応した専用の装置である。

【0019】

各ポータブルデバイス8、9、10は、音楽コンテンツを記憶するための記憶媒体を有している。記憶媒体としては、例えば、装置の内部基板に装着された取り外しが不可能なICメモリや、着脱が可能なメモリカード等が用いられる。ポータブルデバイス8、9、10は、USB等の物理的なインターフェース4を介して各デバイスドライバ13、14及びPDドライバ18と接続され、音楽コンテンツが転送される。このとき、音楽コンテンツは、暗号化及び圧縮された状態で提供され、利用条件情報も付加されている。

【0020】

各ポータブルデバイス8、9、10は、各デバイスドライバ13、14及びPDドライバ18から転送された音楽コンテンツを、各音楽コンテンツに付加された利用条件情報とともに、メモリカード等の記憶媒体内に暗号化して格納する。そして、各ポータブルデバイス8、9、10は、通常、パソコン3との接続が切り離された状態で用いられ、この状態でユーザにより再生命令が与えられると、暗号化した音楽コンテンツを記憶媒体から読み出し、再生をする。また、各ポータブルデバイス8、9、10は、各音楽コンテンツに付加されている利用条件情報に基づき、また、必要に応じて再生の制限を行ったり、音楽コンテンツの削除等の制御を行ったり、利用条件情報の更新等を行う。なお、メモリカード内に格納した音楽コンテンツは、各デバイスドライバ13、14及び包括管理ユニット

(X) 15やポータブルデバイス 8, 9, 10独自の暗号化方式で暗号化されており、また、その圧縮方式や利用条件情報のフォーマットも異なる。そのため、例えば他のデバイスドライバ等と直接接続して、音楽コンテンツを転送することはできないようになっている。

【0021】

購入用アプリケーション(A) 11は、EMDサーバとの接続処理、ログファイル等をアップロードする処理、音楽コンテンツ、コンテンツ鍵及び利用条件情報等をダウンロードする処理等を行う。この購入用アプリケーション(A) 11は、対応しているEMDサーバに対してのみ接続処理を行うようになっている。具体的には、購入用アプリケーション(A) 11は、EMDサーバ(A) 5に対応した処理を行い、他のEMDサーバに対して接続処理を行うことができない。また、購入用アプリケーション(A) 11は、EMDサーバと接続した際の認証処理、ポータブルデバイスと接続した際の認証処理、ハードディスク19に格納している音楽コンテンツ及び利用条件情報の暗号化／暗号解読処理等を行う。購入用アプリケーション(A) 11は、例えば、EMDサーバからダウンロードした音楽コンテンツ及びその利用条件情報をコンテンツ鍵で暗号化し、このコンテンツ鍵をセッション鍵で暗号化して、ハードディスク19に格納する。なお、暗号化処理の方式は、各購入用アプリケーションでそれぞれ独自の方式を採用している。そのため、パソコン3内の同一のハードディスク19に格納されている音楽コンテンツであっても、専用の購入用アプリケーションでなければ、他の購入用アプリケーションでは暗号を解読することができないようになっている。

【0022】

また、購入用アプリケーション(A) 11は、各音楽コンテンツに付加されている利用条件情報の管理も行う。例えば、購入用アプリケーション(A) 11は、利用条件情報に再生回数限度値が記述され、コンテンツの再生回数の制限がされている場合には、再生や複製を行う度に、再生や複製の回数限度値を1回分デクリメントする等の処理を行う。

【0023】

また、購入用アプリケーション(A) 11は、自己がハードディスク19上に

管理している音楽コンテンツ及び利用条件情報を、包括管理ユニット (X) 15 の EMD 用受信インターフェース 16 に送信する。

【0024】

購入用アプリケーション (B) 12 は、EMD サーバとの接続処理、ログファイル等をアップロードする処理、音楽コンテンツ、コンテンツ鍵及び利用条件情報等をダウンロードする処理等を行う。この購入用アプリケーション (B) 12 は、対応している EMD サーバに対してのみ接続処理を行うようになっている。具体的には、購入用アプリケーション (B) 12 は、EMD サーバ (B) 6 に対応した処理を行い、他の EMD サーバに対して接続処理を行うことができない。また、購入用アプリケーション (B) 12 は、EMD サーバと接続した際の認証処理、ポータブルデバイスと接続した際の認証処理、ハードディスク 19 に格納している音楽コンテンツ及び利用条件情報の暗号化／暗号解読処理等を行う。購入用アプリケーション (B) 12 は、例えば、EMD サーバからダウンロードした音楽コンテンツ及びその利用条件情報をコンテンツ鍵で暗号化し、このコンテンツ鍵をセッション鍵で暗号化して、ハードディスク 19 に格納する。

【0025】

また、購入用アプリケーション (B) 12 は、各音楽コンテンツに付加されている利用条件情報の管理も行う。例えば、購入用アプリケーション (B) 12 は、利用条件情報に再生回数限度値が記述され、コンテンツの再生回数の制限がされている場合には、再生や複製を行う度に、再生や複製の回数限度値を 1 回分デクリメントする等の処理を行う。

【0026】

また、購入用アプリケーション (B) 12 は、包括管理ユニット (X) 15 の EMD 用受信インターフェース 16 との間で、自己がハードディスク 19 上に管理している音楽コンテンツ及び利用条件情報を、相互に転送を行う。

【0027】

デバイスドライバ (A) 13 は、音楽コンテンツの再生や、ポータブルデバイス (A) 8 への音楽コンテンツの転送等を行うアプリケーションソフトウェアである。デバイスドライバ (A) 13 は、購入用アプリケーション (A) 11 によ

り管理されている音楽コンテンツや包括管理ユニット (X) 1 5 により管理されている音楽コンテンツの再生を行い、また、ポータブルデバイス (A) 8 にこれらの音楽コンテンツを転送する。また、デバイスドライバ (A) 1 3 は、音楽コンテンツの再生時においては、音楽コンテンツの伸張処理も行う。圧縮伸張処理の方式は、各デバイスドライバでそれぞれ独自の方式を採用している。

【 0 0 2 8 】

デバイスドライバ (B) 1 4 は、音楽コンテンツの再生や、ポータブルデバイス (B) 9 への音楽コンテンツの転送等を行うアプリケーションソフトウェアである。デバイスドライバ (B) 1 4 は、購入用アプリケーション (B) 1 2 により管理されている音楽コンテンツや包括管理ユニット (X) 1 5 により管理されている音楽コンテンツの再生を行い、また、ポータブルデバイス (B) 9 にこれらの音楽コンテンツを転送する。また、デバイスドライバ (B) 1 4 は、音楽コンテンツの再生時においては、音楽コンテンツの伸張処理も行う。

【 0 0 2 9 】

包括管理ユニット (X) 1 5 は、EMDサーバ (X) 7 から音楽コンテンツの提供を受ける音楽提供会社 X 専用のアプリケーションソフトウェアであるとともに、デバイスドライバ (A) 1 3 及びデバイスドライバ (B) 1 4 や、購入用アプリケーション (A) 1 1 及び購入用アプリケーション 1 2 との間で音楽コンテンツ及び利用条件情報の転送を行って、パソコン 3 内の音楽コンテンツを包括的に管理を行う管理ソフトウェアでもある。また、自己が管理を行う音楽コンテンツを、携帯型の音楽再生装置である専用のポータブルデバイス (X) 1 0 に転送することができる。

【 0 0 3 0 】

PD用ドライバ 1 8 は、ポータブルデバイス (X) 1 0 との接続用のインターフェースモジュールで、このポータブルデバイス (X) 1 0 との間における認証処理や暗号化処理を行う。また、PD用ドライバ 1 8 は、他のポータブルデバイス 8, 9 に音楽コンテンツ等を転送する場合には、デバイスドライバ (A) 1 3 やデバイスドライバ (B) 1 4 を介して音楽コンテンツ及び利用条件情報を転送する。

【0031】

EMD用受信インターフェース16は、購入用アプリケーション(A)11からの音楽コンテンツ及び利用条件情報の受信、EMDサーバ(X)7からネットワーク2を介して転送された音楽コンテンツ及び利用条件情報の受信、及び、オーディオプレーヤ(B)12との間での音楽コンテンツ及び利用条件情報の送受信を行う。

【0032】

EMD用受信インターフェース16は、購入用アプリケーション(A)11から音楽コンテンツ及び利用条件情報を受信する場合には、相互認証処理、暗号化方式の変換、転送する音楽コンテンツに付加された利用条件情報のフォーマットの変換、転送する音楽コンテンツの圧縮方式の変換等を行う。暗号化方式、利用条件情報、圧縮方式の変換は、購入用アプリケーション(A)11が用いている方式から、包括管理ユニット(X)15が用いている方式に変換される。ここで包括管理ユニット(X)15が用いている方式を、以下、統一転送プロトコルと呼ぶ。そして、EMD用受信インターフェース16は、このように統一転送プロトコルに変換した音楽コンテンツ及び利用条件情報を、購入用アプリケーション(B)12に送信したり、また、PD用ドライバ18を介してデバイスドライバ(A)13やデバイスドライバ(B)14に送信する。また、EMD用受信インターフェース16は、統一転送プロトコルに変換した音楽コンテンツ及び利用条件情報を、PDドライバ18を介して、ポータブルデバイス(X)10に送信する。

【0033】

また、EMD用受信インターフェース16は、購入用アプリケーション(B)12との間で、音楽コンテンツ及び利用条件情報の送受信を行う。ここで、購入用アプリケーション(B)12は、音楽コンテンツの暗号化方式、利用条件情報のフォーマット、圧縮方式が、上記統一転送プロトコルと同一となっている。したがって、この間では、利用条件情報のフォーマットの変換、転送する音楽コンテンツの圧縮方式の変換は行われない。

【0034】

また、EMD用受信インターフェース16は、購入用アプリケーション(A)11により管理されている音楽コンテンツ、EMDサーバ(X)7からダウンロードした音楽コンテンツを、受信する。ここで、EMDサーバ(X)7は、音楽コンテンツの暗号化方式、利用条件情報のフォーマット、圧縮方式が、上記統一転送プロトコルと同一となっている。したがって、この間では、利用条件情報のフォーマットの変換、転送する音楽コンテンツの圧縮方式の変換は行われな

【0035】

このようなEMD用受信インターフェース16は、EMDサーバ(X)7から音楽コンテンツ及び利用条件情報を受信して購入用アプリケーション12に転送し、また、購入用アプリケーション(A)11から暗号化方式、利用条件情報のフォーマット、圧縮方式が異なる音楽コンテンツを受信してそれを購入用アプリケーション(B)12に転送する。そして、購入用アプリケーション12は、EMDサーバ(A)5、EMDサーバ(B)6、EMDサーバ(X)からダウンロードされたそれぞれのコンテンツ提供会社の音楽コンテンツを統括的に管理を行う。

【0036】

また、EMD用受信インターフェース16は、音楽コンテンツの複製(コピー)、移動(ムーブ)、チェックイン、チェックアウトの機能を有している。

【0037】

EMD用受信インターフェース16は、ユーザからの複製命令、移動命令に従い、例えば、購入用アプリケーション(A)11に格納されている音楽コンテンツを、購入用アプリケーション(B)12に複製や移動する処理を行う。この際に、EMD用受信インターフェース16は、音楽コンテンツの暗号化方式及び圧縮方式、利用条件の記述フォーマットの変換を行って、統一転送プロトコルとする。

【0038】

また、ユーザからのチェックイン命令に従い、コンパクトディスク等の外部メディアやポータブルデバイス8、9、10に格納されている音楽コンテンツを、

購入用アプリケーション (B) 1 2 に複製や移動する処理を行う。この際に、EMD用受信インターフェース 1 6 は、音楽コンテンツの暗号化方式及び圧縮方式、利用条件の記述フォーマットが統一転送プロトコルとされていなければ、これらの変換を行って、統一転送プロトコルとする。

【 0 0 3 9 】

また、ユーザからのチェックアウト命令に従い、購入用アプリケーション (A) 1 1 や購入用アプリケーション (B) 1 2 に格納されている音楽コンテンツを、ポータブルデバイス 1 0 に移動する処理を行う。この際に、EMD用受信インターフェース 1 6 は、音楽コンテンツの暗号化方式及び圧縮方式、利用条件の記述フォーマットが統一転送プロトコルとされていなければ、これらの変換を行って、統一転送プロトコルとする。

【 0 0 4 0 】

また、包括管理ユニット (X) 1 5 では、図 2 に示すように、アプリケーション層の下位レイヤに統一転送プロトコルを設けて、このレイヤにおいて他の購入用アプリケーションとのデータ転送を行っている。そして、包括管理ユニット (X) 1 5 は、この統一転送プロトコルの更に下位レイヤを http として、EMDサーバ (X) 7 とのデータ送受信を行っている。

【 0 0 4 1 】

以上のような構成の音楽コンテンツ配信システム 1 では、EMDサーバ (A) 5 から配信された音楽コンテンツを、デバイスドライバ (A) 1 3 及びポータブルデバイス (A) 8 が取得し、再生を行うようになっている。また、EMDサーバ (B) 6 から配信された音楽コンテンツを、デバイスドライバ (B) 1 4 及びポータブルデバイス (A) 9 が取得し、再生を行うようになっている。また、EMDサーバ (X) 7、EMDサーバ (A) 及び EMDサーバ (B) から配信された音楽コンテンツを、ポータブルデバイス (X) 1 0 が再生を行うようになっている。

【 0 0 4 2 】

以上のように音楽コンテンツ配信システム 1 では、包括管理ユニット (X) 1 5 を中心として、各購入用アプリケーション及びデバイスドライバの間で、転送

する音楽コンテンツの暗号化方式の変換、転送する音楽コンテンツに付加された利用条件情報のフォーマットの変換、転送する音楽コンテンツの圧縮方式の変換が行われ、統一転送プロトコルを用いて音楽コンテンツの相互転送が行われる。そのため、例えば、購入用アプリケーション (A) 1 1 により EMD サーバ (A) 5 からダウンロードした音楽コンテンツを、包括管理ユニット (X) 1 5 を介して購入用アプリケーション (B) 1 2 に転送することができ、このため、例えば音楽提供会社 A からのみ提供されるアーティストの音楽コンテンツを、デバイスドライバ (B) 1 4 やポータブルデバイス (A) 9 やポータブルデバイス (X) 1 0 により再生することができる。すなわち、この音楽コンテンツ配信システム 1 では、音楽コンテンツの暗号化方式、利用条件情報のフォーマット、音楽コンテンツの圧縮方式等を、統一転送プロトコルに変換するので、パソコン 3 のハードディスク内に格納されている様々な方式の音楽コンテンツを、任意の 1 つのオーディオプレーヤやポータブルデバイスにより再生を行うことができる。特に、音楽コンテンツ配信システム 1 では、相互転送の際に、暗号化方式及び利用条件情報を変換するので、音楽コンテンツの著作権の保護を図りつつ、その音楽コンテンツの取り扱いの自由度を大きくすることができる。

【0043】

すなわち、音楽コンテンツ配信システム 1 では、音楽コンテンツの再生や制御を行うオーディオプレーヤ間で、少なくとも暗号化方式と利用条件情報の変換を行って、音楽コンテンツ及び利用条件情報の転送を行う。このことにより、音楽コンテンツ配信システム 1 では、複数のオーディオプレーヤが存在してもパソコン 3 内の例えばハードディスク 1 9 に格納されている音楽コンテンツを自由に移動させることができ、統一的な音楽コンテンツの管理をすることができる。また、音楽コンテンツとともに利用条件情報も転送するので、1 つの音楽コンテンツに対して利用条件が重複したりすることがなく、音楽コンテンツの著作権も確実に保護することができる。

【0044】

(2) 利用条件情報

(一般的に用いられる利用条件情報の説明)

購入用アプリケーション (A) 1 1 に用いられる利用条件情報のフォーマットの一例について説明をする。

【0 0 4 5】

購入用アプリケーション (A) 1 1 では、例えば、図 3 (a) に示すような表形式で記述された利用条件情報が用いられている。

【0 0 4 6】

表の左欄には、利用条件のポリシーが列方向に記述され、右欄には各ポリシーの具体的な値が記述される。例えば、ポリシーとして、再生開始可能日 (f r o m)、再生終了日 (t o)、1 回の再生に対する価格 (p a y / p l a y) 等が記述される。このような利用条件情報は、図 3 (b) に示すように各音楽コンテンツに付加された状態で、EMDサーバ (A) 5 から配信される。購入用アプリケーション (A) 1 1 は、記述されているポリシー及びその値に従い、音楽コンテンツの制御を行う。例えば、利用条件情報に、再生開始可能日 (f r o m) が 9 9 年 1 0 月 2 5 日、再生終了日 (t o) が 9 9 年 1 1 月 2 4 日、1 回の再生に対する価格 (p a y / p l a y) が y e s / 1 0 円と記述されているとする。この場合、その音楽コンテンツは、9 9 年 1 0 月 2 5 日から再生が可能とされ、それ以前にユーザから再生命令があっても、再生を禁止する。また、その音楽コンテンツは、9 9 年 1 1 月 2 4 日まで再生が可能とされ、それ以後となると、その音楽コンテンツを消去する。また、その音楽コンテンツは、1 回の再生の度に 1 0 円の課金を行うように設定されており、例えば、ユーザが再生した回数を別途ログ情報として保管しておき、そのログ情報を EMDサーバ (A) 5 にアップロードして、視聴したユーザに対して視聴した回数分だけの課金処理を行う。

【0 0 4 7】

(包括管理ユニット (X) 1 5 が用いている利用条件情報の説明)

包括管理ユニット (X) 1 5 が用いている利用条件情報について説明する。以下説明をする利用条件情報は、EMDサーバ (X) 7 からダウンロードされる音楽コンテンツに付加されており、上記包括管理ユニット (X) 1 5 がその音楽コンテンツの制御を行う際に用いられる。また、この利用条件情報は、購入用アプリケーション (A) 1 1 と包括管理ユニット (X) 1 5 との間、及び、購入用ア

アプリケーション (A) 1 1 と包括管理ユニット (X) 1 5 との間で、音楽コンテンツの相互転送をする際の統一フォーマットとして用いられる。以下、この利用条件情報を、統一利用条件情報と称する。

【0048】

統一利用条件情報は、図4に示すように、インデックスファイル31、オートマトンファイル32と、パラメータファイル33と、履歴ファイル34とから構成される。各ファイルは、XML言語で記述されている。

【0049】

インデックスファイル31には、各ファイルのリファレンス情報等が記述されている。

【0050】

オートマトンファイル32には、図5に示すように、利用条件がオートマトンで記述されたオートマトン記述部41と、コンテンツ鍵による認証コード (MAC: Message Authentication Code) 42、コンテンツ提供者の署名 (Sig) 43、この署名を検証するための認証書 (Cert) 44 が付加されている。ここで、コンテンツ鍵を K_C 、コンテンツを作成したコンテンツ提供者のプライベート鍵及びパブリック鍵をそれぞれ K_E^{-1} , K_E^1 とする。

【0051】

オートマトン記述部41は、tuple列で記述されたExtended State Machineにより音楽コンテンツの動作状態が記述される。

【0052】

具体的には、オートマトン記述部41では、現在の音楽コンテンツの動作状態の集合を Q とし、音楽コンテンツのイベントを表す入力シンボルの集合を Σ とし、状態遷移した後の音楽コンテンツの動作状態の集合を Q' を以下のように表す。

【0053】

$$Q' = \{d \mid d = \delta(q, \alpha) \mid q \in Q, \alpha \in \Sigma, \delta: Q \times \Sigma \rightarrow Q\}$$

そして、以上の Q , Σ , Q' に基づき、各tupleを

$$\{ \langle q, \alpha, d \rangle \mid q \in Q, d \in Q, \alpha \in \Sigma \}$$

として表す。

【0054】

ここで、 Σ には、再生 (Play) ,複製 (copy) ,支払い金額 (pay Y) ,再生開始可能日時 (from YMD) ,再生終了日時 (to YMD) ,使用可能日数 (in Ddays) ,ヌルイベント (ε) といったイベントが、以下のように記述される。

【0055】

$\Sigma = \{\text{Play}, \text{copy}, \text{pay } Y, \text{from YMD}, \text{to YMD}, \text{in Ddays}, \varepsilon\}$

例えば、オートマトン記述部 4 1 には、図 6 に示すような音楽コンテンツの動作遷移を示すオートマトンを、図 7 に示すようにな tuple 列にして記述する。

【0056】

また、オートマトン記述部 4 1 は、音楽コンテンツの動作を更新するため、動作状態の並列合成を記述しても良い。例えば、動作 a_0 と動作 a_1 との並列合成は、tuple 列で以下のように表される。

【0057】

$\langle q_0, \alpha, a_0. q_0 \rangle$

$\langle q_0, \alpha, a_1. q_0 \rangle$

また、オートマトン記述部 4 1 には、状態遷移に伴うアクションを記述してもよい。例えば、アクションは、tuple で以下のように表される。

【0058】

$\langle q_0, \alpha, q_1; \text{action} \rangle$

このアクションは、予め定義した変数を用いた関数として表される。また、変数は、ID とスコープと初期値とからなる。スコープには、その音楽コンテンツ、アルバム、システム全体等のクラスがある。例えば、アルバム (a) の買い取りの値段を表す変数を n とし、 $a. n := 1000$ のように記述する。このように変数に対するアクションが記述されたオートマトン記述部 4 1 の一例を以下に示す。

【0059】

$\langle q_0, \text{pay } 100, q_1, a. n := a. n - 100 \rangle \quad \dots (1)$

$\langle q_0, \text{pay } (a. n), q_1, a. n := 0 \rangle \quad \dots (2)$

$\langle q_1, \text{play}, q_2 \rangle \dots (3)$

この例は、1つの音楽コンテンツの買い取り値段 {式(1)} が、アルバム買い取り {式(2)} の値段に影響を及ぼすことを示している。

【0060】

以上のようなオートマトン記述部41は、図8に示すように、エントリーID45と、コンテンツID46と、バージョン情報47と、変数情報48と、tuple49列とから構成される。

【0061】

以上のように記述フォーマットが定められたオートマトン記述部41の具体例を図9～図12に示す。なお、以下の図9～図12の記述で用いられているイベントとコマンドとを図13に示す。

【0062】

図9は、音楽コンテンツが1999年9月1日から再生が可能であることを示すXML言語によるオートマトン記述部41の記述例である。

【0063】

図10は、音楽コンテンツが1999年10月31日まで再生が可能であることを示すXML言語によるオートマトン記述部41の記述例である。

【0064】

図11は、音楽コンテンツの再生回数を16回に制限することを示すXML言語によるオートマトン記述部41の記述例である。

【0065】

図12は、音楽コンテンツの再生可能期間が1999年9月1日から1999年10月31日までであって、且つ、その再生可能回数が16回であることを示すXML言語によるオートマトン記述部41の記述例である。

【0066】

図13は、再生動作 (play)、複製動作 (copy)、再生権購入 (pay-for-play)、複製権購入 (pay-for-copy)、アルバム再生権購入 (pay-for-album-play)、アルバム複製権購入 (pay-for-album-copy)、使用可能開始日 (from)、使用終了日 (to)、ヌル動作 (null) がイベントとして設定されている例である。

【0067】

つぎに、パラメータファイル 33 には、図 14 に示すように、パラメータ記述部 51、コンテンツ鍵による認証コード 52、コンテンツ提供者の署名 53、この署名を検証するための認証書 54 が付加されている。ここで、コンテンツ鍵を K_C 、コンテンツを作成したコンテンツ提供者のプライベート鍵及びパブリック鍵をそれぞれ K_E^{-1} 、 K_E^1 とする。

【0068】

また、パラメータファイル 33 は、上記オートマトンファイル 32 を作成したコンテンツ提供者とは別のコンテンツ提供者（例えば、コンテンツ小売業者やコンテンツ中間業者等の二次提供者）により書き換えることが可能である。書き換えられたパラメータファイル 33 は、図 15 に示すように、それぞれの提供者や中間業者等に与えられたユニークなエンティティ ID 55 が付加される。ここで、 K'_C は、二次提供者のコンテンツ鍵で、 $K'_C = H(K_C, EntityID)$ となる。二次提供者のコンテンツ鍵 K'_C は、一次提供者のコンテンツ鍵 K_C から作成される。一次提供者と二次提供者とは、その認証書により区別される。

【0069】

パラメータファイル 33 を検証する方法としては、コンテンツ鍵が得られていれば MAC により行い、安全性等の理由でコンテンツ鍵が得られない場合には署名と証明書により検証する。

【0070】

MAC により検証するプロトコルは以下のようになる。コンテンツの一次提供者を S、二次提供者を A、端末を B とする。

【0071】

$S \rightarrow A : K'_C = H(K_C, ID_A)$

$S \rightarrow B : X = E_{K_S}(K_C)^1$

$A \rightarrow B : ID_A, Parameters, M = MAC_{K'_C}(Parameters)$

$B : M \equiv MAC_{K'_C}(Parameters) ?$

このパラメータ記述部 51 には、上記オートマトンファイル 31 のオートマトン部 41 に記述された値の変更のための関数の係数が記述される。例えば、図 7

に示した例において、オートマトン部 4 1 では、例えば、以下のように音楽コンテンツの価格が関数となる場合がある。

【0072】

$\langle q_0, \text{pay}(f_1(10)), q_1 \rangle$

$\langle q_1, \text{pay}(f_2(10) \times n), q_2 \rangle$

この場合、上記関数 f_1 及び f_2 を、例えば、以下のように定める。

【0073】

$f_1(n) = 0.9n$

$f_2(n) = 90 + 0.1n$

このように関数を定めることによって、例えば、一次提供者が価格のデフォルト値を定め、二次提供者がパラメータファイル 3 3 を書き換えて、価格を変更することができる。

【0074】

以上のようなパラメータ記述部 5 1 は、図 1 6 に示すように、エントリー ID 5 6 と、コンテンツ ID 5 7 と、係数情報 5 8 とから構成される。

【0075】

履歴ファイル 3 4 は、オートマトン記述部 4 1 に記述内容に基づき動作する音楽コンテンツの動作の軌跡を記述するファイルである。上記オートマトン記述 4 1 の `tuple` 内のステータスと変数を記録する。例えば、上述した図 7 に例において、2 回再生を行った場合には、

$\langle q_0, q_1, q_0, q_1 \rangle$

となり、これにより以下のような動作の軌跡を得ることができる。

【0076】

$\langle \text{pay}10, \text{play}, \text{pay}10, \text{play} \rangle$

これを集計して、例えば、包括管理ユニット (X) 1 5 にアップロード等すれば、ユーザの支払い金額を計算することができる。

【0077】

以上のように音楽コンテンツ配信システム 1 では、オートマトンにより利用条件を表現した統一利用条件情報を用いているので、コンテンツの利用条件の記載

の自由度を高めることができる。

【0078】

(3) 破壊された音楽コンテンツ等のリストア及び再ダウンロード

つぎに、包括管理ユニット (X) 15 による音楽コンテンツのバックアップについて説明をする。

【0079】

まず、包括管理ユニット (X) 15 の音楽コンテンツの鍵管理方法について、図 17 を用いて説明する。

【0080】

包括管理ユニット (X) 15 は、パソコン 3 内のハードディスク 19 に、音楽コンテンツ C1, C2, C3...Cn を格納している。また、包括管理ユニット (X) 15 は、各音楽コンテンツ C1, C2, C3...Cn に対応するコンテンツ鍵 Kc1, Kc2, Kc3...Kcn も格納している。コンテンツ鍵 Kc は、音楽コンテンツ C に対して一対一の関係となっている。また、各音楽コンテンツ C1, C2, C3...Cn には、それぞれの識別するためのコンテンツ ID が付加されている。このコンテンツ ID を、CID1, CID2, CID3...CIDn とする。

【0081】

音楽コンテンツ C1, C2, C3...Cn は、コンテンツ鍵 Kc1, Kc2, Kc3...Kcn により暗号化され、E(Kc1, C1), E(Kc2, C2), E(Kc3, C3)...E(Kcn, Cn) とされた状態でパソコン 3 のハードディスク 19 内に記録されている。ここで、E(K, C) は、鍵 K でコンテンツ C を暗号化していることを示す。通常、コンテンツ ID は、音楽コンテンツ C のヘッダなどに記録されて音楽コンテンツ C とともに暗号化されているか、或いは、MAC が音楽コンテンツ C に付加された状態とされており、音楽コンテンツ本体と切り離しができないようになっている。

【0082】

また、コンテンツ鍵 Kc1, Kc2, Kc3...Kcn は、ストレージ鍵 KS により暗号化され、E(SK, Kc1), E(SK, Kc2), E(SK, K

c 3) . . . E (SK, Kcn) とされた状態でパソコン 3 のハードディスク 19 上に記録されている。このストレージ鍵 KS は、いわゆる耐タンパ性を有しており、通常のユーザからは参照することができない記録領域に保存されている。

【0083】

以上のように鍵管理が行われる包括管理ユニット (X) 15 では、例えば、音楽コンテンツ C 1 の再生を行う場合には、ストレージ鍵 KS を用いてコンテンツ鍵 Kc 1 の暗号を解除し、続いて、このコンテンツ鍵 Kc 1 を用いて、音楽コンテンツ C 1 の暗号を解除する。このことにより、包括管理ユニット (X) 15 は、音楽コンテンツ C 1 の再生を行うことができる。

【0084】

また、以上のように鍵管理が行われる包括管理ユニット (X) 15 では、例えば、音楽コンテンツ C 1 をハードディスク 19 からポータブルデバイス (X) 10 に移動 (MOVE) する場合には、ポータブルデバイス (X) 10 との間で相互認証を行い、認証が完了するとストレージ鍵 KS を用いてコンテンツ鍵 Kc 1 の暗号を解除し、続いて、セッション鍵によりコンテンツ鍵 Kc 1 を暗号化し、暗号化したコンテンツ鍵 Kc 1 及び暗号化した音楽コンテンツ C 1 をポータブルデバイス (X) 10 に転送する。そして、コンテンツ鍵 Kc 1 と音楽コンテンツ C 1 をともにハードディスク 19 から消去をする。このことにより、包括管理ユニット (X) 15 は、音楽コンテンツ C 1 をポータブルデバイス (X) 10 に移動することができる。

つぎに、ハードディスク 19 が破壊した場合など、音楽コンテンツやコンテンツ鍵をハードディスク 19 から再生することができなくなったときにおける音楽コンテンツの復元方法について説明する。

【0085】

まず、通常時において、包括管理ユニット (X) 15 は、ハードディスク 19 内に、暗号化した音楽コンテンツ C 及びコンテンツ鍵 Kc のバックアップデータを保存しておく。

【0086】

また、通常時において、包括管理ユニット (X) 15 は、EMDサーバ (X)

7からダウンロードした音楽コンテンツの購入記録と、ハードディスク19内に記憶している全ての音楽コンテンツのコンテンツIDのリストとを、使用ログ情報として管理する。このログ情報は、音楽コンテンツをEMDサーバ(X)7からダウンロードしたときや、ポータブルデバイス(X)10への移動等の音楽コンテンツの制御を行ったときに、更新するようにする。包括管理ユニット(X)15は、このログ情報を、定期的、或いは、アクセスした度に、EMDサーバ(X)7にアップロードする。

【0087】

そして、包括管理ユニット(X)15のハードディスク19に格納されている音楽コンテンツCやコンテンツ鍵Kcが破壊されてしまった場合には、以下に示すような処理が行われる。

【0088】

音楽コンテンツCやコンテンツ鍵Kcが破壊されてしまった場合、包括管理ユニット(X)15は、まず、EMDサーバ(X)7にアクセスを行って、ユーザ認証を行う。

【0089】

続いて、EMDサーバ(X)7は、認証したユーザのユーザIDから、包括管理ユニット(X)15の使用ログ情報を参照して、整合検証値ICV(Integrity Check Value)を生成する。この整合検証値ICVは、使用ログ情報に記述されている音楽コンテンツCのコンテンツIDであるCIDと、包括管理ユニット(X)15のストレージ鍵KSとに基づき、以下のように生成される。

【0090】

$$ICV = H(SK, CID1 || CID2 || \dots || CIDn)$$

ここで、 $H(K, Data)$ は、一方向ハッシュ関数で、鍵Kによりその値が変化するものである。

【0091】

続いて、EMDサーバ(X)7は、生成した整合検証値ICVを、包括管理ユニット(X)15に送信する。

【0092】

続いて、包括管理ユニット (X) 15 は、音楽コンテンツ C 又はコンテンツ鍵 K c がバックアップされていれば、そのバックアップデータをリストアして、音楽コンテンツ C 又はコンテンツ鍵 K c をハードディスク 19 内に保存する。また、音楽コンテンツ C 又はコンテンツ鍵 K c がバックアップされていなければ、EMDサーバ (X) 7 から破壊された音楽コンテンツ C 又はコンテンツ鍵 K c を再配信してもらう。このとき、EMDサーバ (X) 7 は、ユーザの購入履歴を参照して、以前に購入しているコンテンツであれば、課金処理を行わない。

【0093】

包括管理ユニット (X) 15 は、以上の処理を行い、破壊された音楽コンテンツ C 又はコンテンツ鍵 K c を復活させる。

【0094】

そして、包括管理ユニット (X) 15 は、復活された音楽コンテンツ C 又はコンテンツ鍵 K c の再生や制御を行う場合には、上記整合検証値 I C V によりその音楽コンテンツの C I D をチェックするようにする。このように、整合検証値 I C V を用いて復活させた音楽コンテンツ C 又はコンテンツ鍵 K c をチェックすることにより、例えば、ある音楽コンテンツ C i をポータブルデバイス (X) 10 に移動してハードディスク 19 上からは消去されている場合に、悪意のあるユーザが暗号化された音楽コンテンツ C i である $E(K c i, C i)$ を覚えておきリストアしたとしても、それらのデータは再生をすることもまた移動等の制御をすることもできない。

【0095】

なお、音楽コンテンツ C 及びコンテンツ鍵 K c ではなく、ストレージ鍵 S K が破壊されている場合には、包括管理ユニット (X) 15 の再インストールを行う。この場合であっても、EMDサーバ (X) 7 にユーザ登録をするとともにログ情報をアップロードしておけば、上述した方法でリストアや再ダウンロードをすることができる。

【0096】

このように、音楽コンテンツ配信システム 1 では、例えば、ハードディスクの

クラッシュ等により、音楽コンテンツが破壊されてしまった場合であっても、著作権を保護しながら、復元することができる。例えば、その音楽コンテンツが正規に購入したものであれば、無料で復活させることができる。

【0097】

(4) 包括管理ユニットのマスター鍵及び認証鍵等の配布方法

包括管理ユニット (X) 15 とポータブルデバイス (X) 10 との間では、ポータブルデバイス (X) 10 の固有の ID 及び認証鍵 (MG-ID / IK) と、包括管理ユニット (X) 15 の固有のマスター鍵 (OMG-MK) とを用いて、相互認証が行われる。

【0098】

包括管理ユニット (X) 15 とポータブルデバイス (X) 10 との間で、相互認証が行われると、包括管理ユニット (X) 15 からポータブルデバイス (X) 10 へ音楽コンテンツを送信したり、ポータブルデバイス (X) 10 から包括管理ユニット (X) 15 への音楽コンテンツの返却をしたりできるようになる。なお、包括管理ユニット (X) 15 は、パソコン 3 のハードディスク 19 内に暗号化した音楽コンテンツを保存しており、また、ポータブルデバイス (X) 10 は、内部のメモ리카ード等の記憶媒体に暗号化した音楽コンテンツを保存する。そのため、包括管理ユニット (X) 15 からポータブルデバイス (X) 10 へ音楽コンテンツを送信する場合には、パソコン 3 のハードディスク 19 上の音楽コンテンツが、ポータブルデバイス (X) 10 に装着されたメモ리카ード上に転送されることとなる。また、ポータブルデバイス (X) 10 から包括管理ユニット (X) 15 へ音楽コンテンツを送信する場合には、ポータブルデバイス (X) 10 に装着されたメモ리카ード上の音楽コンテンツが、パソコン 3 のハードディスク 19 上に転送されることとなる。

【0099】

ポータブルデバイス (X) 10 は、ID 情報 (MG-ID)、複数世代分の認証鍵 (MG-IK) 及び複数世代分のマスター鍵 (OMG-MK) を予め保持している。ポータブルデバイス (X) 10 には、外部からこれらの鍵等が供給されない。ポータブルデバイス (X) 10 は、必要に応じて、認証鍵 (MG-IK)

及びマスター鍵 (OMG-MK) の世代を更新する。ポータブルデバイス (X) 10 は、世代更新された最も新しい世代の認証鍵及びマスター鍵で相互認証を行い、旧世代の認証鍵及びマスター鍵では、相互認証を行わない。以下、ポータブルデバイス (X) 10 は、第 0 世代から第 99 世代の 100 世代分の認証鍵 (MG-IK [0-99]) 及びマスター鍵 (OMG-MK [0-99]) を保持しているものとする。なお、第 i 世代の認証鍵を (MG-IK [i]) と示し、第 i 世代のマスター鍵を (OMG-MK [i]) と示す。

【0100】

また、包括管理ユニット (X) 15 は、マスター鍵 (OMG-MK) を保持することによって、オーディオ用コンパクトディスク等からパソコン 3 内に音楽コンテンツを転送して、保存することができる。また、包括管理ユニット (X) 15 は、マスター鍵 (OMG-MK) を保持することによって、EMD サーバ (X) 7 から音楽コンテンツをダウンロードして、パソコン 3 内に保存することができる。

【0101】

ここで、包括管理ユニット (X) 15 では、コンパクトディスクから音楽コンテンツを転送することはできるが EMD サーバ (X) 7 からは音楽コンテンツをダウンロードすることができないマスター鍵 (OMG-MK) と、コンパクトディスクからも EMD サーバ (X) 7 からも音楽コンテンツを転送することができるマスター鍵 (OMG-MK) とが異なったものとなっている。以下、コンパクトディスクから音楽コンテンツを転送することはできるが EMD サーバ (X) 7 からは音楽コンテンツをダウンロードすることができない鍵のことを、リッピング専用鍵ともいい、コンパクトディスクからも EMD サーバ (X) 7 からも音楽コンテンツを転送することができる鍵のことを EMD 鍵ともいう。

【0102】

なお、本例では、第 0 世代のマスター鍵 (OMG-MK [0]) がリッピング専用鍵となっており、第 1 世代以後のマスター鍵 (OMG-MK [1~99]) が EMD 鍵となっている。

【0103】

つぎに、リッピング専用鍵を用いた処理の手順について説明する。

【0104】

包括管理ユニット (X) 15 が CD-ROM からインストールされる場合には、図 18 に示すように、包括管理ユニット (X) 15 のインストールソフトウェアが格納された CD-ROM 51 とともに、ポータブルデバイス (X) 10 と、フロッピーディスク 52 とが例えばセットで販売される。フロッピーディスク 52 には、ポータブルデバイス (X) 10 の ID 情報 (MG-ID)、第 0 世代の認証鍵 (MG-IK [0])、第 0 世代のマスター鍵 (OMG-MK [0]) が格納されている。

【0105】

続いて、販売されたポータブルデバイス (X) 10 等を使用可能とするには、まず、CD-ROM 51 をパソコン 3 に装着する (ステップ S11)。続いて、この CD-ROM 51 から包括管理ユニット (X) 15 をパソコン 3 にインストールする (ステップ S12)。すると、包括管理ユニット (X) 15 がパソコン 3 のハードディスク内に格納されることとなる (ステップ S13)。続いて、フロッピーディスク 52 に格納されているポータブルデバイス (X) 10 の ID 情報 (MG-ID) と、第 0 世代の認証鍵 (MG-IK [0]) と、第 0 世代のマスター鍵 (OMG-MK [0]) とをパソコン 3 に保存する (ステップ S14)。

【0106】

このことによって、包括管理ユニット (X) 15 は、音楽 CD 53 等により提供される音楽コンテンツを、パソコン 3 のハードディスク内に格納することができるようになる (ステップ S15)。なお、第 0 世代のマスター鍵 (OMG-MK [0]) は、リッピング専用鍵なので、EMD サーバ (X) 7 から音楽コンテンツをダウンロードできないようになっている。

【0107】

また、ポータブルデバイス (X) 10 は、世代更新がされていく 100 世代分の認証鍵及びマスター鍵を内部に保持しているが、初期設定状態では、第 0 世代

とされている。このため、第0世代の認証鍵及びマスター鍵を保持している包括管理ユニット(X)15と、ポータブルデバイス(X)10との相互認証が可能となる。したがって、音楽CD53等により提供される音楽コンテンツを、ポータブルデバイス(X)10のメモリーカードに格納することができるようになる(ステップS16)。

【0108】

一方、包括管理ユニット(X)15がネットワークを介して提供される場合には、図19に示すように、ポータブルデバイス(X)10とともに、インターネット上のWeb54のアドレス、ユーザID及びパスワード等が提供される。

【0109】

続いて、販売されたポータブルデバイス(X)10等を使用可能とするには、まず、ユーザID及びパスワードを用いてネットワーク上のWeb54にアクセスをする(ステップS21)。続いて、Web54は、ユーザID及びパスワードの認証を行う(ステップS22)。続いて、認証に問題がなければ、Web54は、包括管理ユニット(X)15のインストールソフトウェアと、ポータブルデバイス(X)10のID情報(MG-ID)と、第0世代の認証鍵(MG-IK[0])と、第0世代のマスター鍵(OMG-MK[0])とを、パソコン3に送信する(ステップS23)。続いて、パソコン3は、包括管理ユニット(X)15のインストールソフトウェアを起動して、包括管理ユニット(X)15をインストールするとともに、ポータブルデバイス(X)10のID情報(MG-ID)と、第0世代の認証鍵(MG-IK[0])と、第0世代のマスター鍵(OMG-MK[0])とをハードディスク19に保存する(ステップS24)。すると、ハードディスクには、包括管理ユニット(X)15が格納されることとなる(ステップS25)。

【0110】

このことによって、包括管理ユニット(X)15は、音楽CD53等により提供される音楽コンテンツを、パソコン3のハードディスク19内に格納することができるようになる(ステップS26)。なお、第0世代のマスター鍵(OMG-MK[0])は、リッピング専用鍵なので、EMDサーバ(X)7から音楽コ

ンテンツをダウンロードできないようになっている。

【0111】

また、ポータブルデバイス (X) 10 は、世代更新がされていく 100 世代分の認証鍵及びマスター鍵を内部に保持しているが、初期設定状態では、第 0 世代とされている。このため、第 0 世代の認証鍵及びマスター鍵を保持している包括管理ユニット (X) 15 と、ポータブルデバイス (X) 10 との相互認証が可能となる。したがって、音楽 CD 53 等により提供される音楽コンテンツを、ポータブルデバイス (X) 10 のメモリカード内に格納することができるようになる (ステップ S27)。

【0112】

なお、以上の図 18 及び図 19 に示した方法に限られず、包括管理ユニット (X) 15 及びリッピング専用の第 0 世代のマスター鍵 (OMG-MK [0]) を CD-ROM 51 に格納しておき、ポータブルデバイス (X) 10 との認証用の ID 及び第 0 世代の認証鍵 (MG-ID / IK) をネットワークを介して提供しても良い。

【0113】

つぎに、リッピング専用鍵を EMD 鍵に鍵に更新して、EMD サーバ (X) 7 からダウンロードした音楽コンテンツを取り扱えるようにする処理の手順について説明する。

【0114】

包括管理ユニット (X) 15 は、図 18 又は図 19 に示した手順により、CD-ROM 等のリムーバブルメディアやインターネット等のネットワークを介して提供され、パソコン 3 内のハードディスク 19 にインストールされている。このとき包括管理ユニット (X) 15 は、リッピング専用である第 0 世代のマスター鍵 (OMG-MK [0]) と、認証用の ID 及び第 0 世代の認証鍵 (MG-ID / IK [0]) とを保持しており、ポータブルデバイス (X) 10 の鍵の世代もデフォルトのままである。

【0115】

まず、パソコン 3 は、図 20 に示すように、ユーザ ID 及びパスワードを用い

てネットワーク上のWeb 54にアクセスをする(ステップS31)。続いて、Web 54は、ユーザID及びパスワードの認証を行う(ステップS32)。続いて、認証に問題がなければ、Web 54は、パソコン3のID情報(OMG-ID)を登録し、包括管理ユニット(X)15がEMDサーバ(X)7と接続するための公開鍵(OMG-PK)、秘密鍵(OMG-SK)及び公開鍵の認証書(Cert [PK])を生成する(ステップS33)。続いて、Web 54は、生成した公開鍵(OMG-PK)、秘密鍵(OMG-SK)及び公開鍵の認証書(Cert [PK])を、パソコン3に送信する(ステップS34)。

【0116】

続いて、Web 54は、ポータブルデバイス(X)10のID情報(MG-ID)、第*i*世代の認証鍵(MG-IK [*i*])、第*i*世代のマスター鍵(OMG-MK [*i*])をパソコン3に送信する(ステップS35)。続いて、パソコン3の包括管理ユニット(X)15は、受信したID情報(MG-ID)、第*i*世代の認証鍵(MG-IK [*i*])、第*i*世代のマスター鍵(OMG-MK [*i*])に基づき、これらの鍵を第*i*世代に世代更新する(ステップS36)。続いて、包括管理ユニット(X)15は、ポータブルデバイス(X)10との間で認証を行う(ステップS37)。ポータブルデバイス(X)10は、認証がされると、自己の鍵の世代を第*i*世代に更新する(ステップS38)。

【0117】

このことによって、包括管理ユニット(X)15は、音楽CD53等により提供される音楽コンテンツを、パソコン3のハードディスク内に格納することができるとともに、EMDサーバ(X)7からダウンロードした音楽コンテンツをパソコン3のハードディスク19に格納することができるようになる(ステップS39)。

【0118】

つぎに、EMD鍵等の世代更新をする手順について説明する。

【0119】

包括管理ユニット(X)15は、第*i*世代のマスター鍵(OMG-MK [*i*])と、認証用のID及び第0世代の認証鍵(MG-ID / IK [*i*])とを保持

しており、ポータブルデバイス (X) 10 の鍵の世代も第 i 世代となっている。

【0120】

まず、図 21 に示すように、パソコン 3 が何らかの処理のため、Web 54 にアクセスすると、Web 54 は、包括管理ユニット (X) 15 の ID を認証して、第 $(i+k)$ 世代の認証鍵 (MG-IK $[i+k]$) 及び第 $(i+k)$ 世代のマスター鍵 (OMG-MK $[i+k]$) をパソコン 3 に送信する (ステップ S41)。続いて、パソコン 3 の包括管理ユニット (X) 15 は、受信した認証鍵及びマスター鍵を、第 $(i+k)$ 世代に更新する (ステップ S42)。続いて、包括管理ユニット (X) 15 は、ポータブルデバイス (X) 10 と認証を行う (ステップ S43)。ポータブルデバイス (X) 10 は、認証がされると、自己の鍵の世代を第 i 世代から第 $(i+k)$ 世代に更新する (ステップ S44)。

【0121】

また、図 22 に示すように、一方、ポータブルデバイス (X) 10 が用いている認証鍵等の世代が第 $(i+k)$ 世代となっており、包括管理ユニット (X) 15 が保持している認証鍵等の世代が第 i 世代となっている場合には、ポータブルデバイス (X) 10 と包括管理ユニット (X) 15 との認証が行われると、認証失敗となる (ステップ S51)。認証を失敗すると、包括管理ユニット (X) 15 は、Web 51 に対して、鍵要求を行う (ステップ S52)。鍵要求があると、Web 54 は、包括管理ユニット (X) 15 の ID を認証して、第 $(i+k)$ 世代の認証鍵 (MG-IK $[i+k]$) 及び第 $(i+k)$ 世代のマスター鍵 (OMG-MK $[i+k]$) を送信する (ステップ S53)。続いて、包括管理ユニット (X) 15 は、受信した認証鍵及びマスター鍵を、第 $(i+k)$ 世代に更新する (ステップ S54)。続いて、包括管理ユニット (X) 15 は、ポータブルデバイス (X) 10 と認証を行う (ステップ S55)。

【0122】

このことによって、包括管理ユニット (X) 15 は、音楽 CD 53 等により提供される音楽コンテンツを、パソコン 3 のハードディスク内に格納することができるとともに、EMD サーバ (X) 7 からダウンロードした音楽コンテンツをパソコン 3 のハードディスク 19 に格納することができるようになる (ステップ S3

8)。

【0 1 2 3】

以上のように、音楽コンテンツ配信システム 1 では、包括管理ユニット (X) 1 5 及びポータブルデバイス (X) 1 0 が用いるマスター鍵及び認証鍵を、リッピング専用の鍵とサーバ接続鍵とに分け、さらに、サーバ接続鍵をネットワークを介してダウンロードするようにしている。このため、音楽コンテンツ配信システム 1 では、サーバから配信された音楽コンテンツの安全性が高まり、例えば、リッピング専用の鍵が破られたとしても、サーバからダウンロードされる音楽コンテンツを破ることができない。

【0 1 2 4】

また、音楽コンテンツ配信システム 1 では、包括管理ユニット (X) 1 5 及びポータブルデバイス (X) 1 0 が用いるマスター鍵及び認証鍵を、世代更新させて用いている。さらに、包括管理ユニット (X) 1 5 は、マスター鍵及び認証鍵がネットワークを介して供給され、世代更新を行う。このため、音楽コンテンツの安全性が高まる。

【0 1 2 5】

【発明の効果】

本発明にかかるコンテンツ提供システム及びコンテンツ提供方法では、再生プログラムが、外部記憶媒体に格納されたコンテンツデータのみを取り扱う場合には、第 1 の認証鍵及び第 1 のマスター鍵を用いて、外部記憶媒体に格納されたコンテンツデータの保存及び可搬再生装置との認証を行う。再生プログラムが、ネットワークを介して提供されたコンテンツデータを取り扱う場合には、第 1 の認証鍵及び第 1 のマスター鍵を用いて、外部記憶媒体に格納されたコンテンツデータの保存及び可搬再生装置との認証を行う。第 2 の認証鍵及び第 2 のマスター鍵は、ネットワークを介して再生プログラムに提供され、第 1 の認証鍵及び第 1 のマスター鍵と異なる鍵となっている。

【0 1 2 6】

このことにより、本発明では、ネットワークを介して配信されたコンテンツデータの安全性を高めることができる

【図面の簡単な説明】

【図 1】

本発明の実施の形態の音楽コンテンツ配信システムのシステム構成図である。

【図 2】

統一転送プロトコルレイヤとアプリケーションレイヤとの関係を説明する図である。

【図 3】

一般的に用いられる利用条件情報のフォーマットを説明する図である。

【図 4】

包括管理ユニットで用いられる統一利用条件情報を構成するファイルを説明する図である。

【図 5】

上記統一利用条件情報のオートマトンファイルの構成を説明する図である。

【図 6】

上記オートマトンファイルのオートマトン記述部に記述される音楽コンテンツの動作遷移を示すオートマトンの一例を説明する図である。

【図 7】

上記オートマトンを `t u p l e` 列で表現した図である。

【図 8】

上記オートマトン記述部の構成を説明する図である。

【図 9】

上記オートマトン記述部の第 1 の記述例を示す図である。

【図 1 0】

上記オートマトン記述部の第 2 の記述例を示す図である。

【図 1 1】

上記オートマトン記述部の第 3 の記述例を示す図である。

【図 1 2】

上記オートマトン記述部の第 4 の記述例を示す図である。

【図 13】

上記図 9～図 12 の記述で用いられているイベントとコマンドとを設定した記述例を示す図である。

【図 14】

上記統一利用条件情報のパラメータファイルの構成を説明する図である。

【図 15】

上記パラメータファイルを更新した場合の構成を説明する図である。

【図 16】

上記パラメータファイルのパラメータ記述部の構成を説明する図である。

【図 17】

上記包括管理ユニットによるコンテンツの管理方法について説明する図である。

【図 18】

包括管理ユニットが CD-ROM からインストールされる場合の処理手順について説明する図である。

【図 19】

包括管理ユニットがネットワークからダウンロードされてインストールされる場合の処理手順について説明する図である。

【図 20】

リッピング鍵から EMD 鍵に更新する更新手順について説明する図である。

【図 21】

EMD 鍵を更新する手順の第 1 の例について説明する図である。

【図 22】

EMD 鍵を更新する手順の第 2 の例について説明する図である。

【符号の説明】

1 音楽コンテンツ配信システム、2 ネットワーク、3 パーソナルコンピュータ、4 インターフェース、5, 6, 7 EMDサーバ、8, 9, 10 ポータブルデバイス、11, 12 購入用アプリケーション、13, 14 デバイスドライバ、15 包括管理ユニット、16 EMD用受信インターフェース、

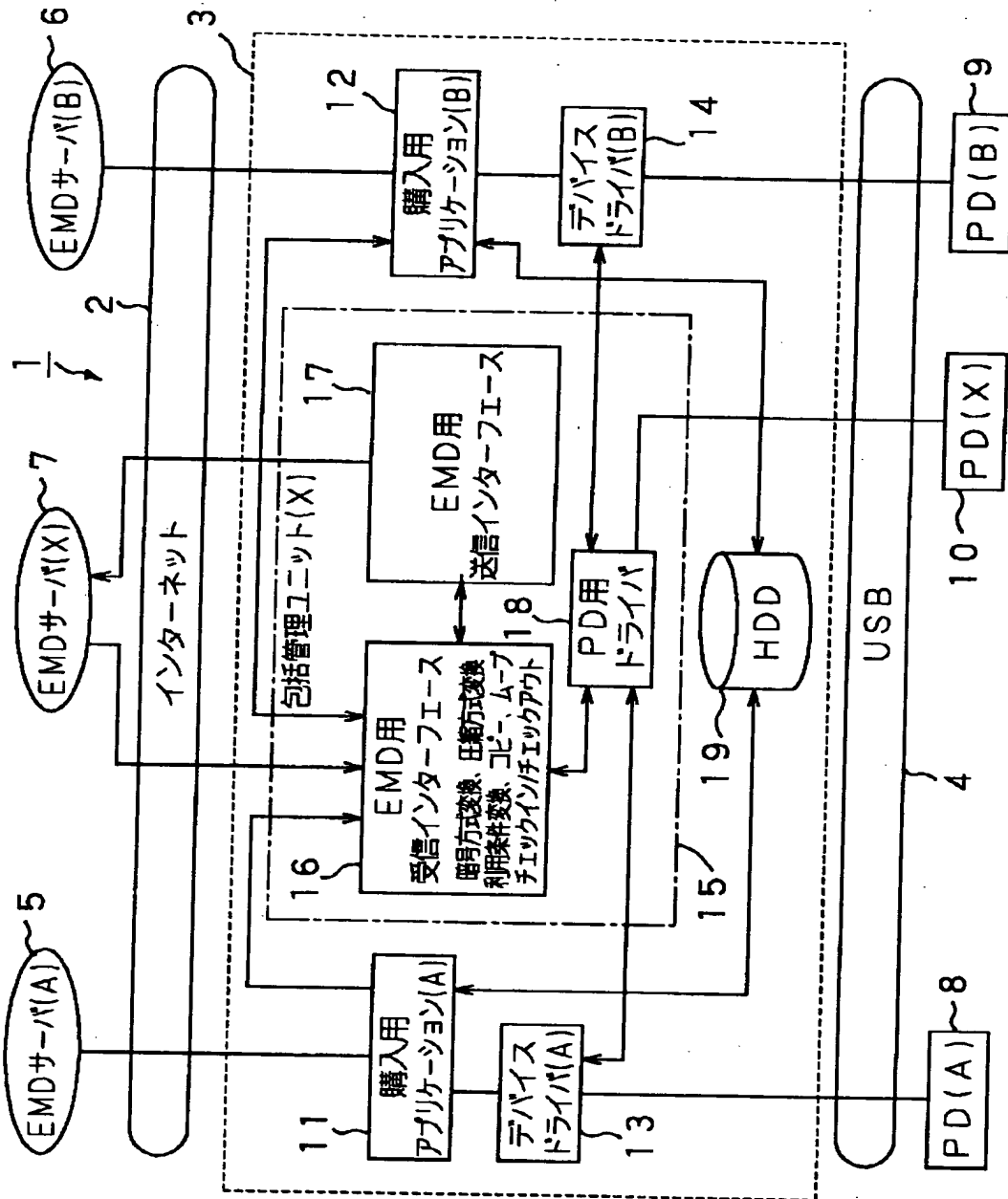
特平 11-303142

17 EMD用送信インターフェース、18 PDドライバ、19 ハードディスク

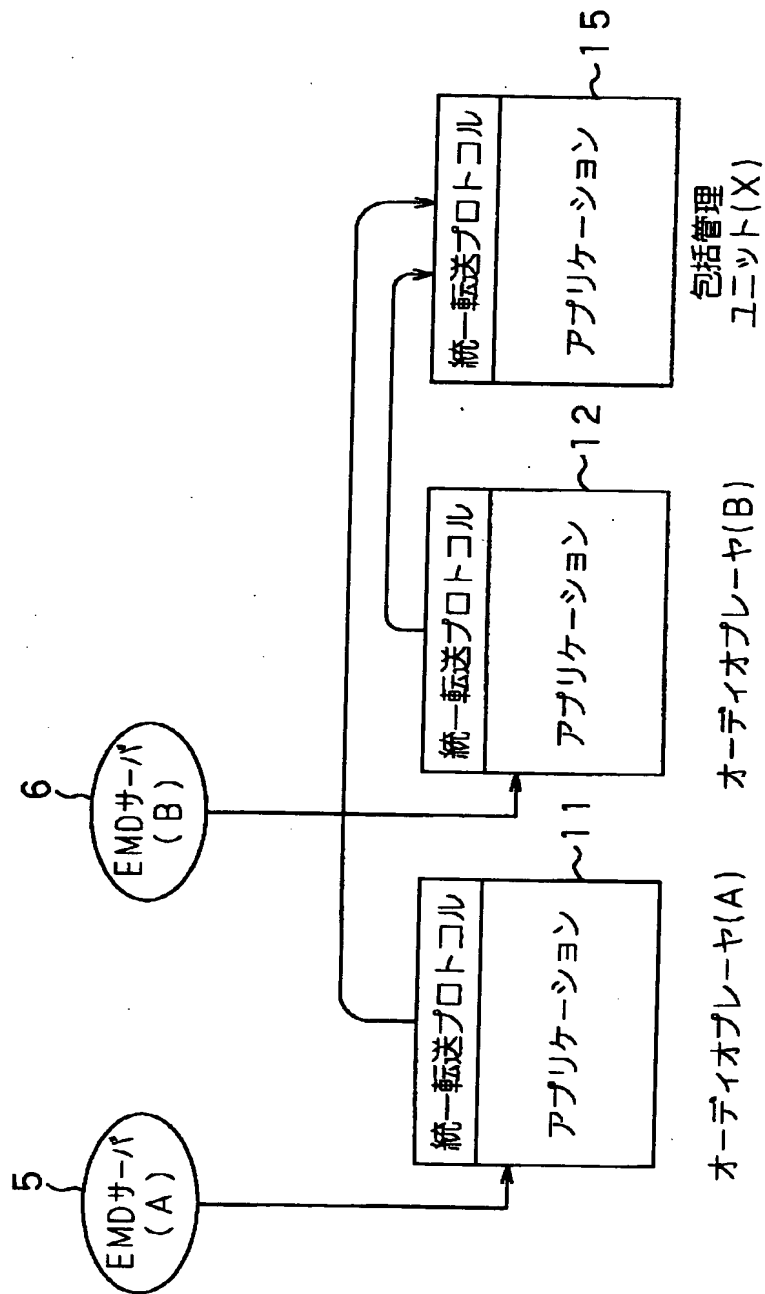
【書類名】

図面

【図 1】



【図 2】



【図 3】

(a)

ポリシー	値
from	99/10/25
to	99/11/24
pay/play	yes/10円

(b)

コンテンツ
利用条件情報

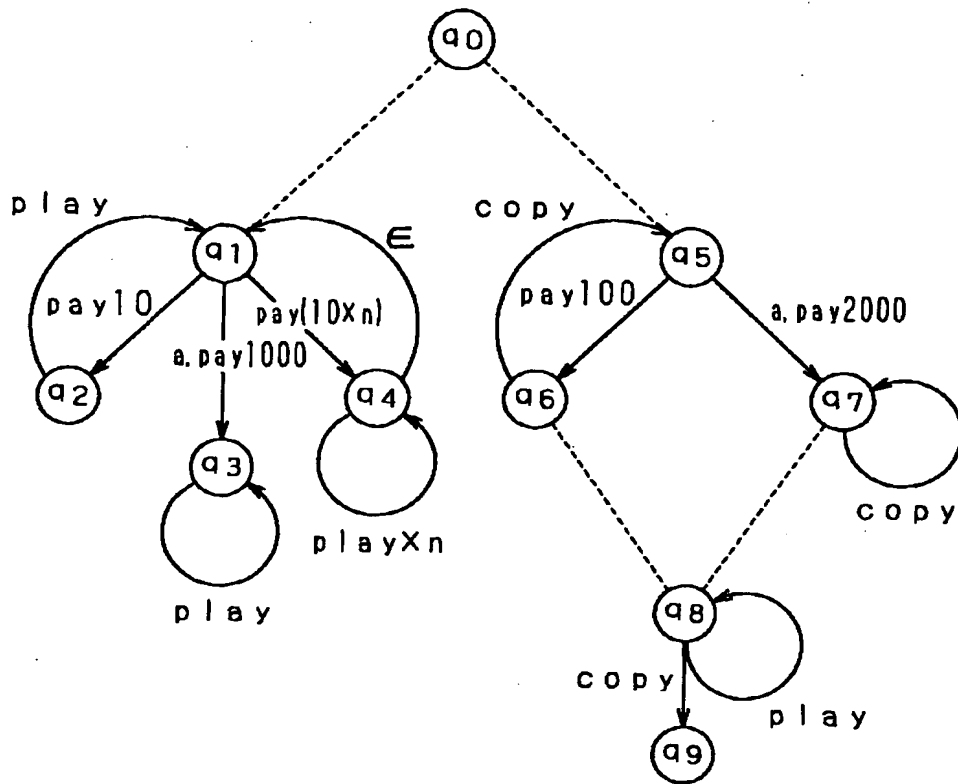
【図 4】

インデックスファイル	~ 31
オートマトンファイル	~ 32
パラメータファイル	~ 33
履歴ファイル	~ 34

【図 5】

Automaton	~ 41
$MAC_{K_C}(\text{Automaton})$	~ 42
$Sig_{K_E}^{-1}(\text{Automaton})$	~ 43
$Cert(K_E^1)$	~ 44

【図 6】



【図 7】

$\langle q_1, \text{pay}10, q_2 \rangle$
 $\langle q_1, a.\text{pay}1000, q_3 \rangle$
 $\langle q_1, \text{pay}(10 \times n), q_4 \rangle$
 $\langle q_2, \text{play}, q_1 \rangle$
 $\langle q_3, \text{play}, q_3 \rangle$
 $\langle q_4, \text{play} \times n, q_4 \rangle$
 $\langle q_4, \epsilon, q_1 \rangle$
 $\langle q_5, \text{pay}100, q_6 \rangle$
 $\langle q_5, a.\text{pay}2000, q_7 \rangle$
 $\langle q_6, \text{copy}, q_5 \rangle$
 $\langle q_7, \text{copy}, q_7 \rangle$
 $\langle q_8, \text{play}, q_8 \rangle$
 $\langle q_8, \text{copy}, q_9 \rangle$

【図 8】

Entity ID	~ 45
Content ID	~ 46
Automaton Version	~ 47
Variables	~ 48
Tuples	~ 49
Automaton Version	~ 47
Variables	~ 48
Tuples	~ 49
⋮	

【図 9】

Content playable from 1999/9/1

```

<automaton>

<!-- This usage rule system has one Right Unit. Initial state is q1 -->
<initial-right-unit state="q1" />

<node state="q1">
  <!-- If after 1999/9/1, transfer to q2 -->
  <rule event="from" next-state="q2">
    <arguments>
      <integer value="time:19990901" />
    </arguments>
  </rule>
</node>

<node state="q2">
  <!-- Playable -->
  <rule event="play" next-state="q2" />
</node>

</automaton>

```

【図 10】

Content playable until 1999/10/31

```

<automaton>

<!-- This Usage Rule System has one Right Unit. Initial state is q2 -->
<initial-right-unit state="q2" />

<node state="q2">
  <!-- If after 1999/10/31, transfer to end -->
  <rule event="to" next-state="end">
    <arguments>
      <integer value="time:19991031" />
    </arguments>
  </rule>

  <!-- Playable -->
  <rule event="play" next-state="q2" >
  </rule>
</node>

<!-- Unusable state -->
<node state="end" />

</automaton>

```

【図 1 1】

Content playable less than and/or equal to 16 times

<automaton>

<!--Define valuable counter for playable numbers. Initial value is 16 -->
<define-variable name="count" initial-value="16" />

<!-- Usage Rule System has one Right Unit. Initial state is q2 -->
<initial-right-unit state="q1" />

<node state="q2">

<rule event="play" next-state="q2" >

<!--"Count" number of times playable -->

<arguments>

<variable name="count" />

<command name="load" />

</arguments>

<!--If this rule is selected, "count" number decrements by one-->

<action>

<variable name="count" />

<command name="load" />

<integer value="1" />

<command name="subtract" />

<variable name="count" />

<command name="store" />

</action>

</rule>

</node>

</automaton>

【図 1 2】

Content playable 16 times from 1999/9/1 to 1999/10/31

```
<automaton>

  <!--Define counter variables for playable numbers. Initial value is 16 -->
  <define-variable name="count" initial-value="16" />

  <!--This Usage Rule System has one Right Unit. Initial state is q1 -->
  <initial-right-unit state="q1" />

  <node state="q1">
    <!--From 1999/9/1 transfer to q2 -->
    <rule event="from" next-state="q2">
      <arguments>
        <integer value="time:19990901" />
      </arguments>
    </rule>
  </node>

  <node state="q2">
    <!--From 1999/10/31. transfer to end -->
    <rule event="to" next-state="end" >
      <arguments>
        <integer value="time:19991031" />
      </arguments>
    </rule>

    <rule event="play" next-state="q2" >
      <!--Playable only for "count" numbers -->
      <arguments>
        <variable name="count" />
        <command name="load" />
      </arguments>
      <!--If this rule is selected, the "count" number decrements by one-->
      <action>
        <variable name="count" />
        <command name="load" />
        <integer value="1" />
        <command name="subtract" />
        <variable name="count" />
        <command name="store" />
      </action>
    </rule>
  </node>

  <!--Unusable state-->
  <node state="end" />

</automaton>
```


【図 1 3】

```
<!ENTITY % event "(
    play
    copy
    pay-for-play
    pay-for-copy
    pay-for-album-play
    pay-for-album-copy
    from
    to
    null
)">
```

```
<!ENTITY % command "(
    drop
    dup
    swap
    add
    subtract
    multiply
    divide
    remainder
    upper
    lower
    equal
    less
    greater
    less-equal
    greater-equal
    and
    or
    not
    bit-and
    bit-or
    bit-xor
    bit-not
)">
```

【図 1 4】

Parameters	~51
MAC _{K_c} (Parameters)	~52
Sig _{K_E} ⁻¹ (Parameters)	~53
Cert(K _E ¹)	~54

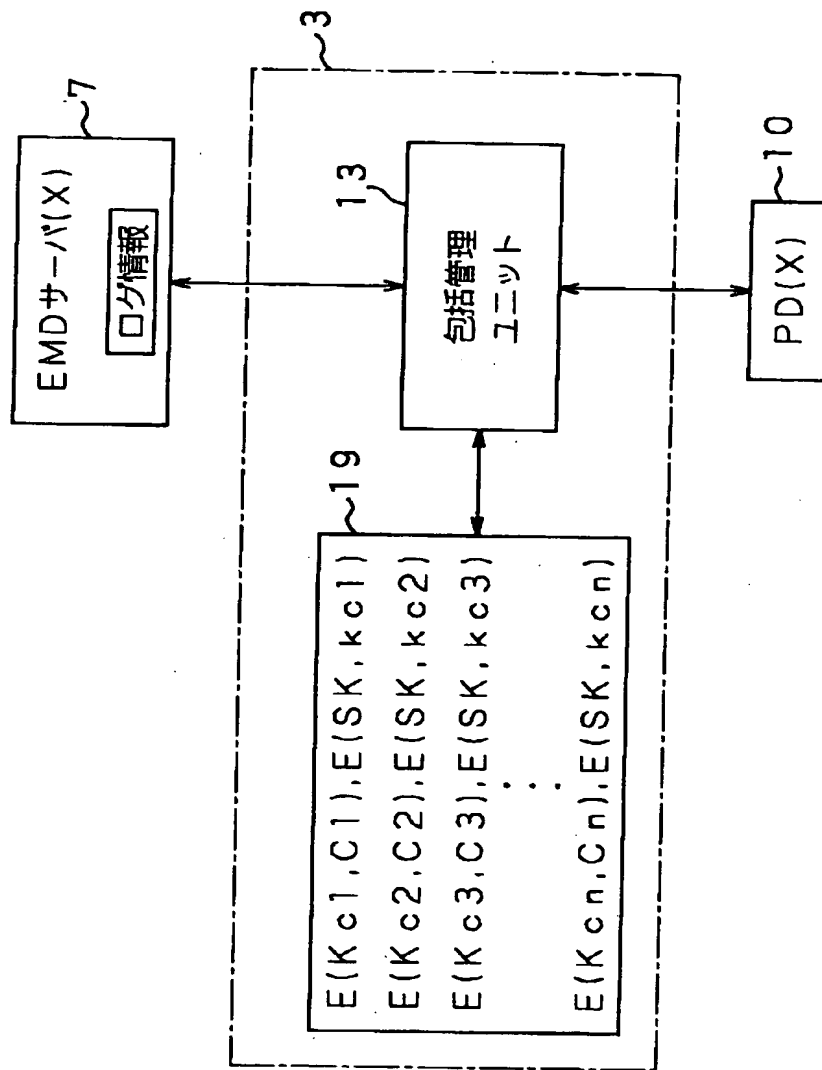
【図 15】

Parameters	~ 51
Entity ID	~ 55
$MAC_{K_C}(Parameters)$	~ 52
$Sig_{K_E^{-1}}(Parameters)$	~ 53
$Cert(K_E^1)$	~ 54

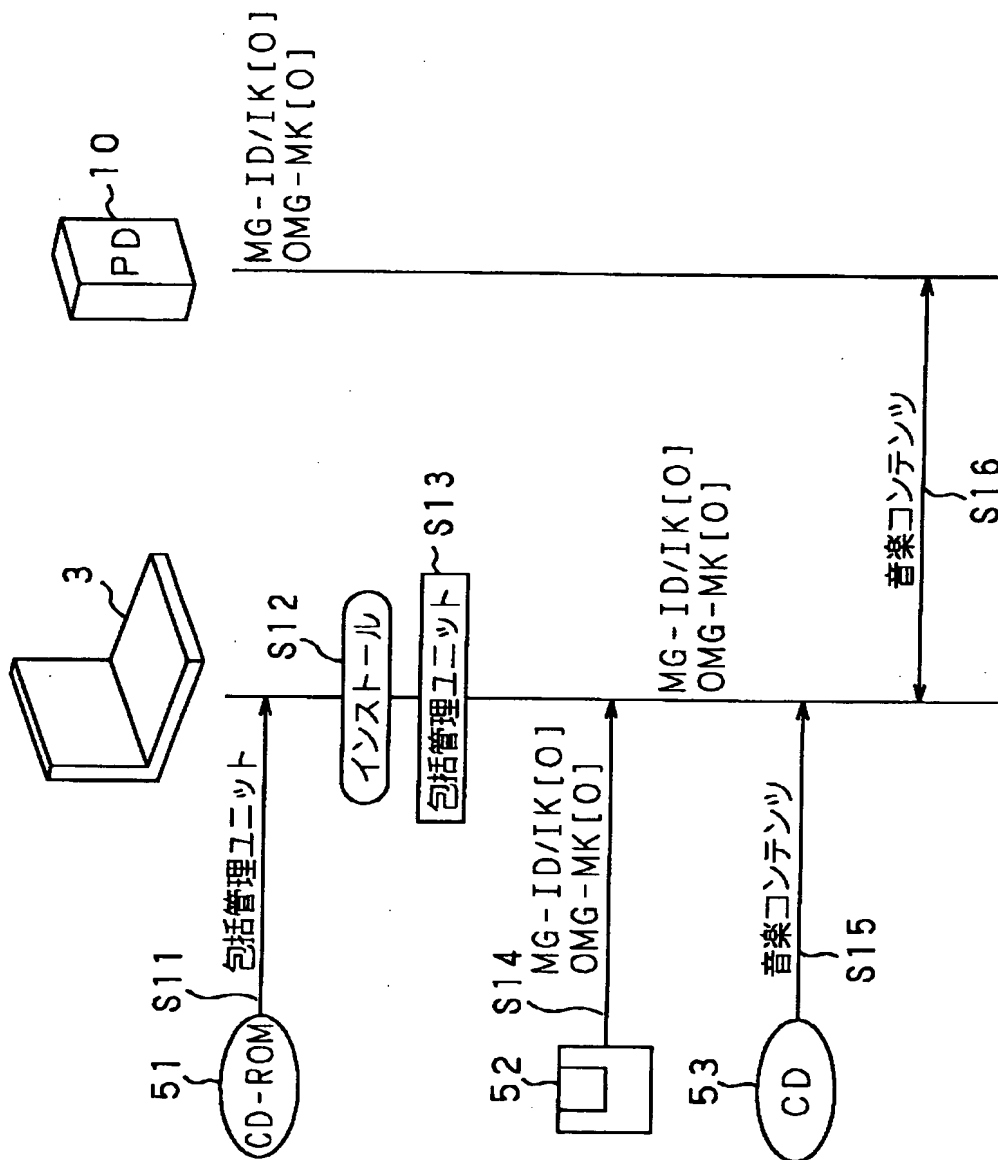
【図 16】

Entity ID	~ 56
Coefficients ID	~ 57
Coefficients	~ 58

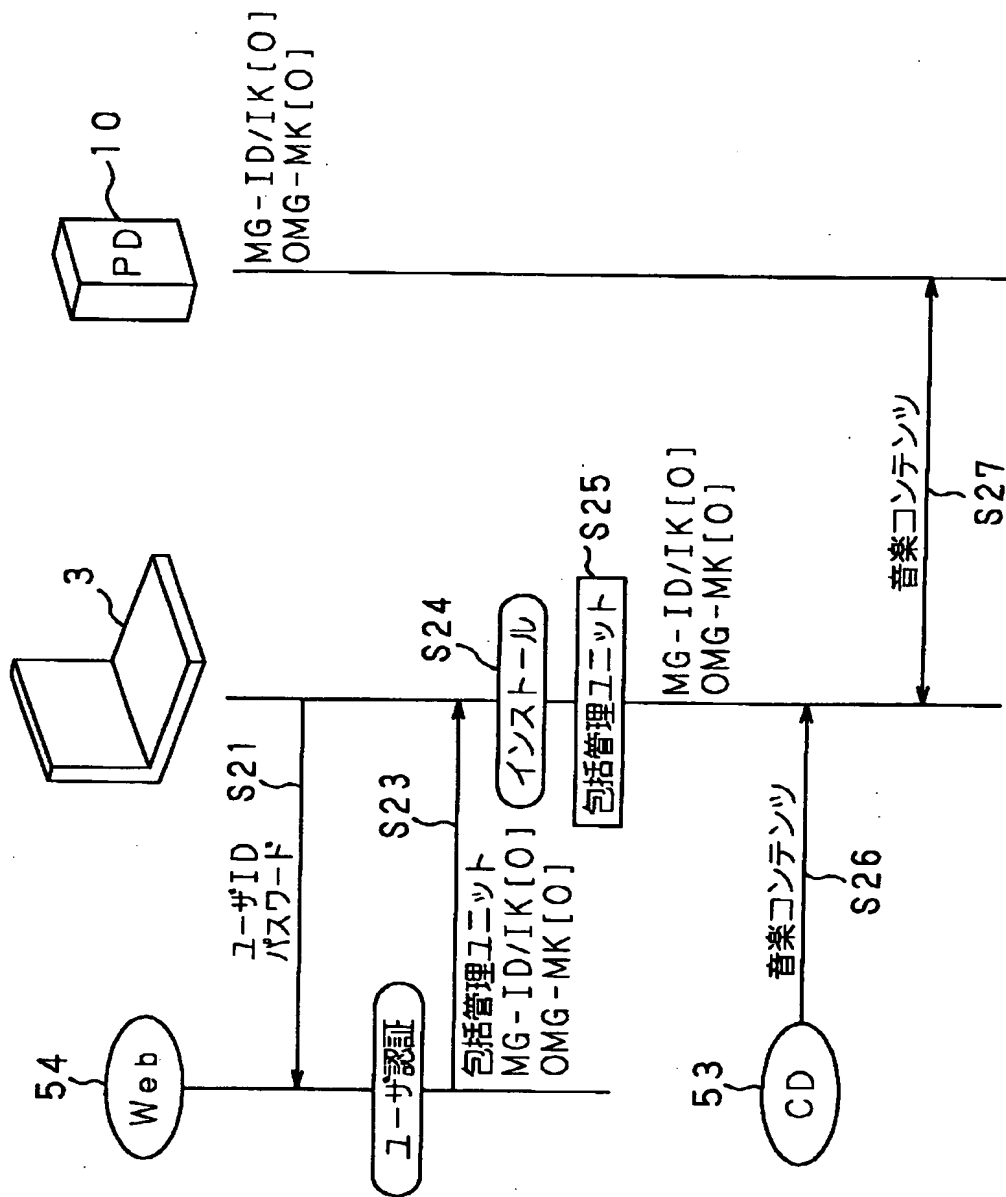
【図 1 7】



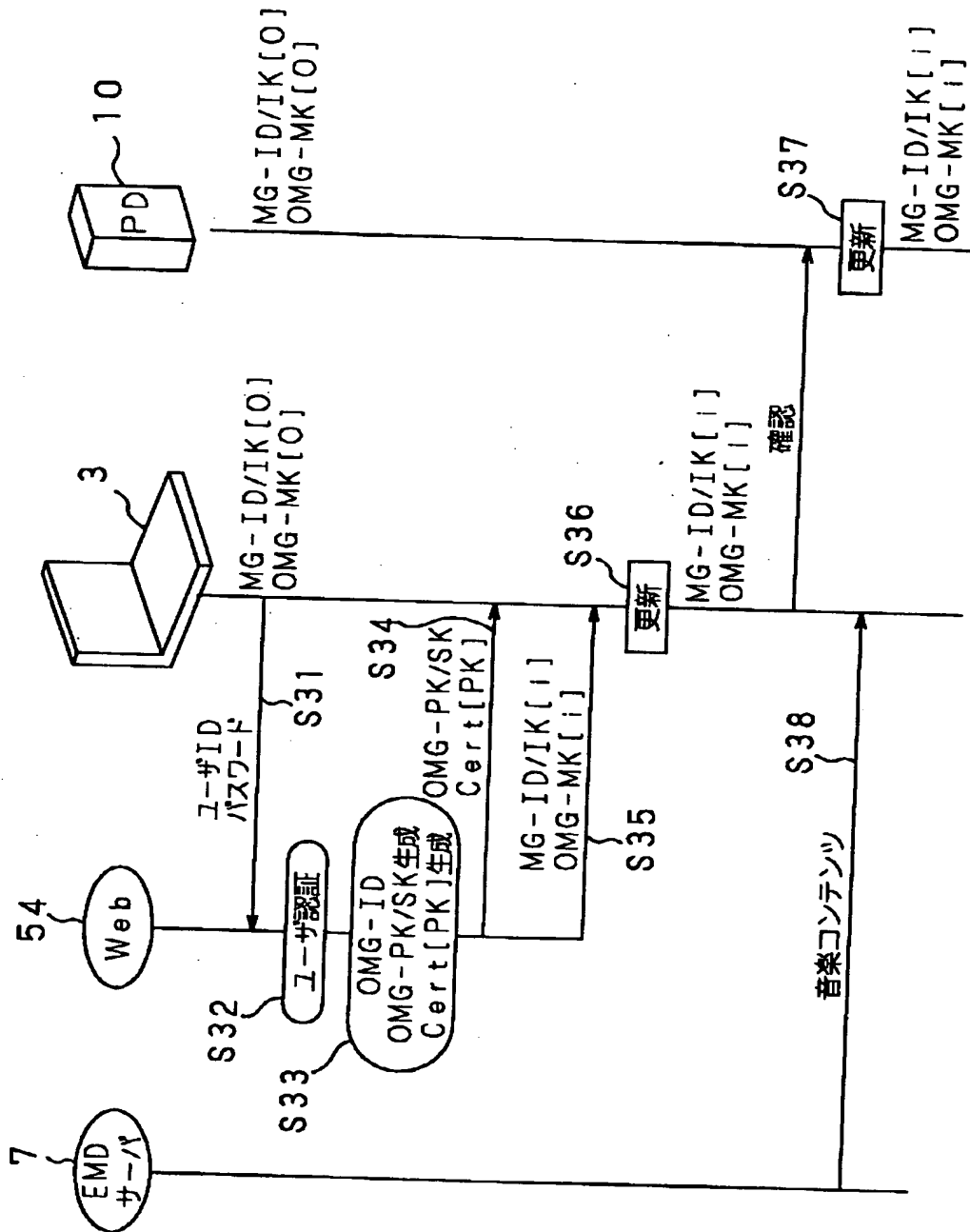
【図 1 8】



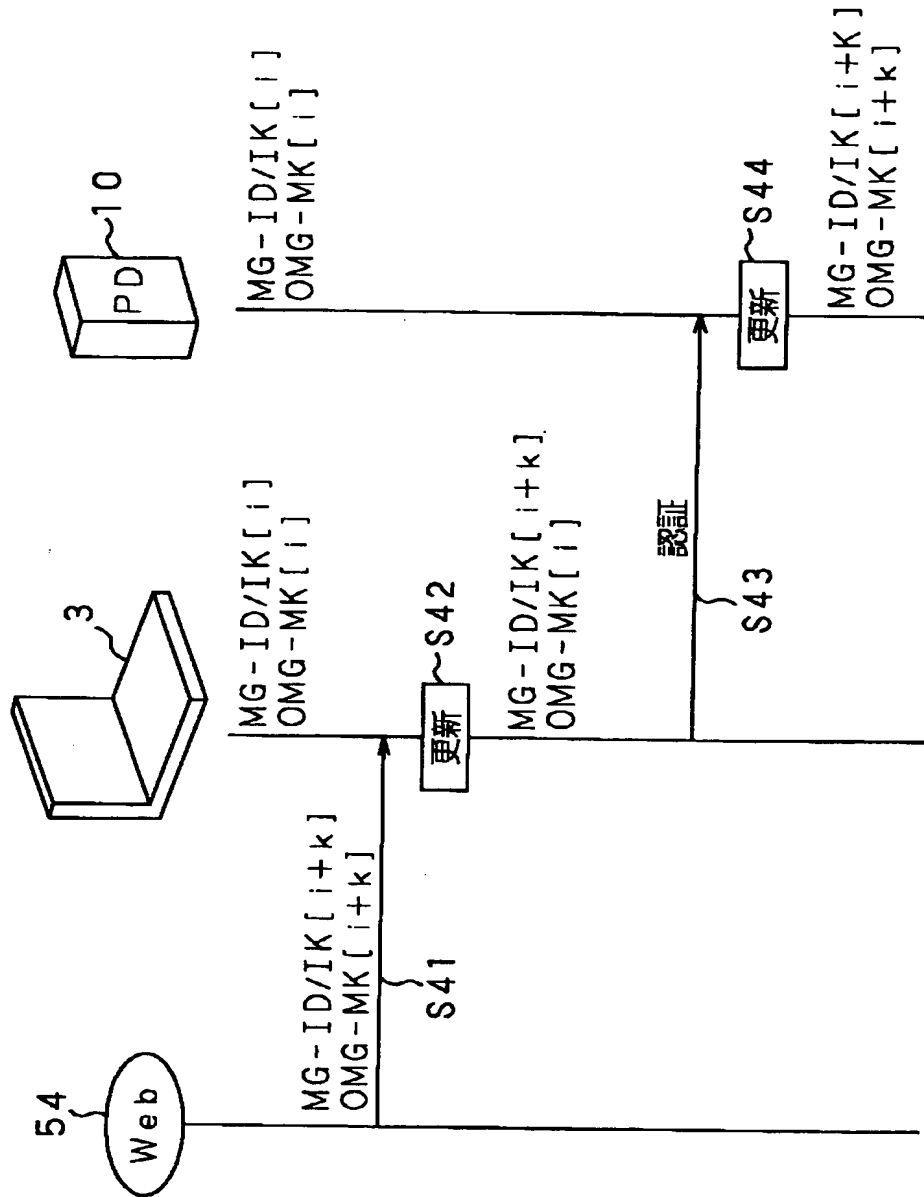
【図 1 9】



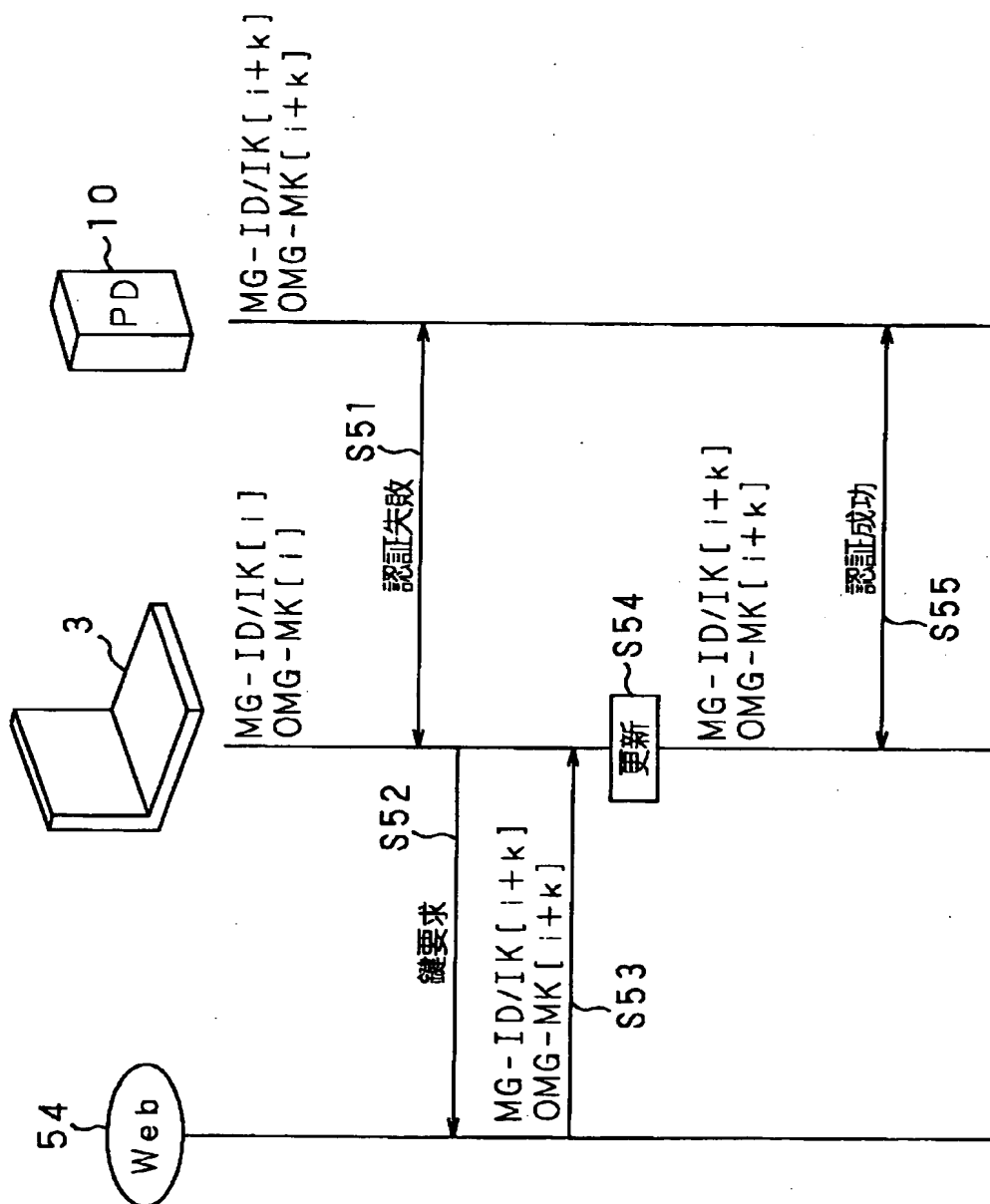
【図 20】



【図 2 1】



【図 2 2】



【書類名】 要約書

【要約】

【課題】 ネットワークを介して配信されたコンテンツデータの安全性を高める

【解決手段】 再生プログラムは、P C上にインストールされた後に、C Dのリッピング用の鍵が例えばF Dから提供される。このC Dのリッピング用の鍵では、C D内の音楽コンテンツをP Dにコピーはできるが、E M Dサーバから音楽コンテンツをダウンロードしてP Dにコピーすることはできない。再生プログラムは、E M Dサーバから配信された音楽コンテンツをP Dに保存する場合には、リッピング用の鍵とは異なるE M D用の鍵をネットワークを介して取得したのちに行う。

【選択図】 図 2 0

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都品川区北品川6丁目7番35号
氏 名	ソニー株式会社